2019-12

INTEGRATION OF SITUATIONAL AWARENESS TOOLS IN THE FIGHT AGAINST UNMANNED AERIAL SYSTEMS

Davis, Brandon R.; Whittaker, William G.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTEGRATION OF SITUATIONAL AWARENESS TOOLS IN THE FIGHT AGAINST UNMANNED AERIAL SYSTEMS

by

Brandon R. Davis and William G. Whittaker

December 2019

Thesis Advisor:	Alex Bordetsky
Co-Advisor:	Leo J. Blanken
Second Reader:	Steven J. Mullins

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE INTEGRATION OF SITUATIONAL AWARENESS TOOLS IN THE FIGHT AGAINST UNMANNED AERIAL SYSTEMS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brandon R. Davis and William G. Whittaker	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In Syria, reports of Islamic State (ISIS) fighters utilizing small unmanned aerial systems (SUAS) to attack U.S. troops and their Syrian Democratic Forces (SDF) partners became a prevalent tactic. Failing to implement meaningful solutions to detect and counter this new application of SUASs by adversaries will cost American lives. The purpose of this project is to research and analyze the current capability gap in situational awareness technology, specifically focused on the integration of counter-UAS (C-UAS) sensors. Using the existing Tactical Assault Kit (TAK) situational awareness tool and developmental applications like the Defense Innovation Unit's Dowding C-UAS System, the project explores solutions to these shortfalls by testing software solutions for integrating UAS sensors. Through field experiments with Norwegian SOF operators in collaboration with DoD partners, this project answers the question, "How can tactical situational awareness tools best enhance decision making and survivability of SOF teams in a threat UAS environment?" The researchers propose the development of a Dowding-based TAK plug-in capable of incorporating data from multiple sensors into a single common operating picture and recommends more rigorous, comprehensive testing of current C-UAS capabilities.

14. SUBJECT TERMS UAS, UAV, mission command, counter-UAS, ATAK, TAK, integration, C-UAS, Drone, detection, acoustics, threat, DIU, Dowding server, protection, sensors, SOF, Special Operations Forces	**15. NUMBER OF PAGES** 119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

INTEGRATION OF SITUATIONAL AWARENESS TOOLS IN THE FIGHT AGAINST UNMANNED AERIAL SYSTEMS

Brandon R. Davis
Major, United States Army
BS, U.S. Military Academy, 2008

William G. Whittaker
Major, United States Army
BS, Gonzaga University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Approved by: Alex Bordetsky
Advisor

Leo J. Blanken
Co-Advisor

Steven J. Mullins
Second Reader

Kalev I. Sepp
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In Syria, reports of Islamic State (ISIS) fighters utilizing small unmanned aerial systems (SUAS) to attack U.S. troops and their Syrian Democratic Forces (SDF) partners became a prevalent tactic. Failing to implement meaningful solutions to detect and counter this new application of SUASs by adversaries will cost American lives. The purpose of this project is to research and analyze the current capability gap in situational awareness technology, specifically focused on the integration of counter-UAS (C-UAS) sensors. Using the existing Tactical Assault Kit (TAK) situational awareness tool and developmental applications like the Defense Innovation Unit's Dowding C-UAS System, the project explores solutions to these shortfalls by testing software solutions for integrating UAS sensors. Through field experiments with Norwegian SOF operators in collaboration with DoD partners, this project answers the question, "How can tactical situational awareness tools best enhance decision making and survivability of SOF teams in a threat UAS environment?" The researchers propose the development of a Dowding-based TAK plug-in capable of incorporating data from multiple sensors into a single common operating picture and recommends more rigorous, comprehensive testing of current C-UAS capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3D	three-dimensional
ADAPT	Advanced Digital Advisor Partner Technologies
ADP	Army Doctrine Publication
AGL	above ground level
AO	area of operations
API	application program interface
APK	Android package
AR	augmented reality
ASCII	American Standard Code for Information Interchange
ATAK	Android Tactical Assault Kit
ATP	Army Technique Publication
AWG	Asymmetric Warfare Group
C2	command and control
CACTF	Combined Arms Collective Training Facility
CBRN	chemical, biological, radiological, and nuclear
CCDC	Combat Capabilities Development Command
CENETIX	Center for Network Innovation and Experimentation
CMP	Collaborative Mission Planner
COP	common operating picture
CoT	cursor-on-target
COTS	commercial off the shelf
CREW	counter remote controlled improvised explosive device electronic warfare
CRUSER	Consortium for Robotics and Unmanned Systems Education and Research
C-UAS	counter-unmanned aerial system
CWMD	countering weapons of mass destruction
DHCP	dynamic host configuration protocol
DiDEX	Defense-in-Depth Exercise
DIU	Defense Innovation Unit

DIU-RS	Defense Innovation Unit-Rogue Squadron
DTRA	Defense Threat Reduction Agency
EHF	extremely high frequency
EUD	end user device
FFI	Norwegian Defence Research Establishment
FMCW	frequency modulated continuous wave
GCS	ground control station
GMTI	ground moving target indicator
GMV	ground mobility vehicle
GPS	global positioning system
GUI	graphical user interface
IED	improvised explosive device
IEEE	Institute of Electrical and Electronics Engineers
ISIS	Islamic State in Iraq and al-Sham
JIDO	Joint Improvised Threat Defeat Organization
JOC	joint operations center
JOCTAK	Joint Operations Center Tactical Assault Kit
LCMR	lightweight counter-mortar radar
LOS	line of sight
LSS	low, slow, small
LTE	Long Term Evolution
MANET	mobile ad hoc network
MDV	minimum detectable velocity
MEMS	micro-electromechanical systems
MJK	Marinejegerkommandoen
MPU	man portable unit
MSL	mean sea level
NATO	North Atlantic Treaty Organization
NGA	National Geospatial-Intelligence Agency
NORSOF	Norwegian Special Operations Forces
NORSOCOM	Norwegian Special Operations Command
NTV	non-tactical vehicle

RAA	Remote Advise and Assist
RCS	radar cross-section
RF	radio frequency
SA	situational awareness
SDF	Syrian Democratic Forces
SDIA	SkyView-Dowding integration application
SIM	sensor interface module
SNMP	simple network management protocol
SNR	signal to noise ratio
SOF	Special Operations Forces
SOF-OC	Special Operations Forces Operating Concept
SUAS	small unmanned aerial system
TAK	Tactical Assault Kit
TAK-Civ	Tactical Assault Kit civilian version
TCP	transmission control protocol
TOC	tactical operations center
TTP	tactic, technique, and procedure
UAS	unmanned Aerial System
UDP	user datagram protocol
UHF	ultra-high frequency
UI	user interface
USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USSOCOM	United States Special Operations Command
USSOF	United States Special Operations Forces
VBIED	vehicle-borne improvised explosive device
VEO	violent extremist organization
VTAK	Virtual Reality Tactical Assault Kit
WAP	wireless access point
WinTAK	Windows Tactical Assault Kit
WLAN	wireless local area network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Dr. Alex Bordetsky, COL (Ret.) Steve Mullins, and Dr. Leo Blanken for their mentorship, guidance, and perseverance throughout the process. From designing the experiments to developing a practical plan and transforming a year's worth of work into a coherent written document, your support and expertise were invaluable. Without your help, we would still be drafting research questions!

We would like to express our gratitude to LtCol Mark Jacobsen and the entire DIU-Rogue Squadron team for making this project possible. Rather than resting on your technology's current capabilities, you willfully pushed it well outside of its intended purpose in the name of progress. You regularly stepped away from other duties to troubleshoot errors, code entire new applications, and redesign entire sections of the Dowding System for problems that only applied to our project. Your sacrifices to make this happen do not go unnoticed.

We would also like to thank LTC Matt McKee at USASOC G8, Mark Rosenberg at DTRA, Mike Bray at AWG, and Mike Stevens from the NPS CORE lab for sharing our passion to enable the warfighter and for helping us resource and design this project.

To the men of the MJK, thank you for the opportunity to conduct these tests with true warriors. Your support, feedback, and recommendations were incredibly germane and critical to our project. We give special thanks to Knut for his tireless efforts to wrangle the ever-changing requirements of our experiments. Skål!

To Maj Andrew Walker, who did all of the work required to complete a thesis without any of the credit. Thank you for helping us "stretch the mesh" and for treating our project like it was your own.

Lastly, and most importantly, we thank our families for their patience and support:

Mary Whitney, Parker, Reagan, and Maddox. You brought much-needed diversion from the grind of this endeavor. Thank you for tolerating the long days and keeping me grounded. I love you.

To Grace and Evelyn, thank you for the smiling faces and hugs that made me look forward to coming home every day … and, also for your patience while these Rangers accomplished their mission. I love you!

I. INTRODUCTION

"Sooner or later, everything old is new again," wrote horror writer Stephen King, referring to the human tendency to reuse old concepts and portray them as new.[1] With that quote in mind, imagine the horror of being an American infantryman on today's battlefield and observing a toy drone that can be purchased at Wal-Mart drop a grenade onto your position. The appearance of inexpensive, small unmanned aerial system (SUAS) technology employed as an air support platform, combined with a grenade and a little ingenuity, has made an old threat new again. Air supremacy theorists would argue that American forces have not had an enemy aerial weapon dropped on their positions since Korea.[2] Yet, in 2017, reports surfaced of Islamic State in Iraq and al-Sham (ISIS) fighters using SUAS to attack U.S. troops and their Syrian Democratic Forces (SDF) partners in Syria.[3] The U.S. was not the only target of modified SUAS as the Russians too became victims of drone attacks in Syria.[4] Even unarmed SUAS can compromise U.S. movements, positions, and subsequent targeting of enemy forces, by using drones as an aerial reconnaissance platform. Failing to implement meaningful controls to detect and counter this new application of SUAS by adversaries will cost American lives.

In an effort to combat this emerging threat, the U.S. military has repurposed many of its legacy systems to focus on the SUAS threat, including the Lightweight Counter-Mortar Radar (LCMR) and Q-36 Firefinder counterbattery system. Finding these options sub-optimal, the Department of Defense is pouring billions of dollars into the research and development of counter-UAS (C-UAS) technologies, including $1.5 billion in 2018.[5] Compared to the $200

---

[1] Stephen King, *The Colorado Kid* (New York: Dorchester Publishing Co., 2005), 45.

[2] Peter Grier, "April 15, 1953," *Air Force Magazine,* June, 2011, 55, http://www.airforcemag.com/MagazineArchive/Documents/2011/June%202011/0611april.pdf

[3] Thomas Gibbons-Neff, "ISIS Drones Are Attacking U.S. Troops and Disrupting Airstrikes in Raqqa, Officials Say," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say.

[4] "Russian Airbase Attacked by Drones in Syria," CNN, August 16, 2018, video, 1:46, https://www.cnn.com/videos/world/2018/08/16/drone-attacks-russian-forces-aleppo-syria-pleitgen-lkl-vpx.cnn.

[5] Philip Butterworth-Hayes, "Special Report - U.S. Department of Defense Spending on Counter-UAS Reaches USD 1.5 Billion in 2018," *Unmanned Airspace* (blog), November 4, 2018, https://www.unmannedairspace.info/counter-uas-systems-and-policies/special-report-us-department-defense-spending-counter-uas-reaches-usd-1-5-billion-2018/.

million spent prior to 2018, the DoD's massive spending increase acknowledged the shortcomings in detection and interdiction of enemy UAS.[6]

This increase in spending had enabled C-UAS technological advances to be rapidly fielded in an effort to temporarily fill the protection gap. Deployed service members are being armed with a multitude of C-UAS technologies aimed at both detection and interdiction of enemy UAS. Additionally, Special Operations Forces (SOF) are already equipped with the Android Tactical Assault Kit (ATAK) as their primary situational awareness (SA) tool. Despite the effort to enhance protection for service members through equipment fielding, the DoD has been unable to seamlessly integrate these disparate C-UAS technologies. For the decentralized SOF team operating in an austere environment, many of the C-UAS sensors are neither portable nor integrated into an SA tool. Without SA tool integration, independent C-UAS sensors do not adequately provide the SOF team with the information required to support decision making when faced with an adversary who employs SUAS.

A. PURPOSE

While there have been significant advances in C-UAS technologies in recent years, American ground forces remain vulnerable to the effects of enemy SUAS, especially armed SUAS. The purpose of this project is to research and analyze the current capability gap in situational awareness technology, specifically focused on C-UAS sensor and SA tool integration. Using the existing TAK and the Defense Innovation Unit's (DIU) developmental Dowding C-UAS situational awareness tools, the project explores solutions to this shortfall by evaluating software applications for existing C-UAS sensors. An integrated SA tool and C-UAS system would enable ground forces to detect enemy SUAS, alert the team, and provide additional situational awareness to higher command elements through a predefined communications architecture. Using server-based processing algorithms, this data could then be refined and returned to the ground force. This entire process would be completed in near real-time and without active inputs from either the team on the ground or their command element. Figure 1 shows the project's integrated SA tool concept.

[6] Butterworth-Hayes.

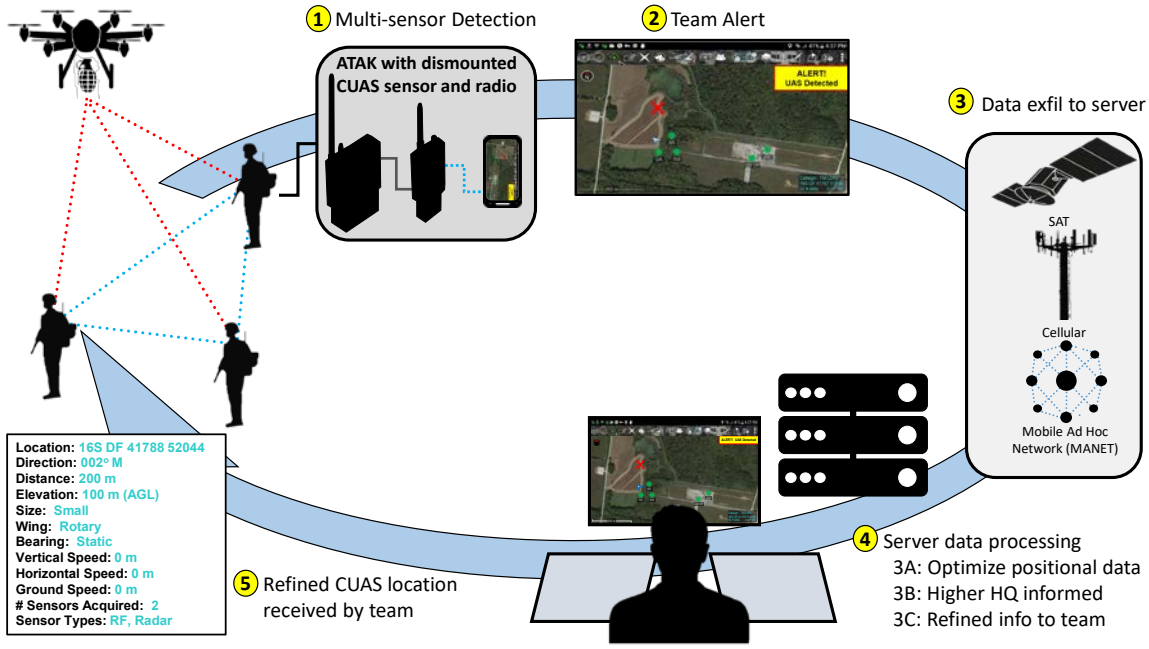


Figure 1. Integrated SA Tool/C-UAS System Concept

The intended audience is the Defense Threat Reduction Agency's (DTRA) Counter Improvised Threat Technologies Department, who is responsible for the rapid acquisition of material solutions to new and improvised threats, and the U.S. Special Operations Command (USSOCOM) G8, who owns the TAK program of record and can prioritize and pursue a solution. Many of the available sensors capable of integrating with situational awareness systems require additional processing and do not directly integrate with the SA tools. Directly networked C-UAS sensors would improve detection and provide limited direction finding of threat SUAS at a small cost and high efficiency. The integration of sensors into the TAK system would provide improved situational awareness, enabling forces to employ active C-UAS measures to enhance lethality and to save lives.

B. RESEARCH OBJECTIVES

The objectives of this research are to identify, evaluate, and prioritize the factors that provide SOF teams, conducting missions while under a C-UAS threat, with the situational awareness required to make informed tactical decisions. The study seeks to answer the following research question:

- How can tactical situational awareness tools enhance decision making and survivability of SOF teams in an enemy SUAS-enabled environment?

And supporting research questions:

- What factors affect the ATAK user interface (UI) usability in support of C-UAS situational awareness?
- What factors affect the Dowding App UI usability in support of C-UAS situational awareness?

This study examines capability gaps and potential utility of select C-UAS sensors, and suggests how those sensors could integrate into the ATAK or Dowding C-UAS systems. This is accomplished through an iterative series of experiments and software development by DIU, culminating in a field test, to evaluate the ATAK and Dowding systems in ground and maritime environments. The result is a prioritized list of findings and recommendations for an integrated SA tool pursuing the following:

- Identify end user requirements for dismounted C-UAS sensor integration or plug-in application
- Determine network requirements for supporting the C-UAS SA tool in the context of an independently operating and decentralized SOF team
- Envision how SOF would use the system to increase situational awareness and survivability

C. SCOPE

This research examines existing commercial off the shelf (COTS) C-UAS technologies and how their integration into selected SA tools could enhance the mission command and protection capability of SOF units in the contemporary operating environment. For this research, the identified threat is low, slow, small (LSS) UAS, specifically commercially available drones. Table 1 depicts UAS group characteristics of which groups 1-3 represent LSS UAS. The research explores the capabilities and drawbacks of current UAS detection

technologies, examines the C-UAS capabilities of different SA tools, and identifies the SOF-specific requirements for SA tools. The experiments use the TAK and the developmental Dowding C-UAS system as the primary test mechanisms. These SA tools, integrated with C-UAS sensors and tactical mobile ad hoc networks (MANET), are field tested in demanding environments by small teams of NATO SOF operators, and provide valuable insights and recommendations for future development. The research does not address larger UAS, such as group 4-5 drones, and focuses exclusively on detection, rather than drone defeat capabilities.

Table 1. UAS Groups 1 through 5[7]

Group	Weight / Altitude	Description
Group 1 Micro / Mini UAS	Weighs 20 pounds or less and normally operates below 1,200 feet above ground level (AGL) at speeds less than 100 knots	These systems are generally hand launched including hobby type UAS. They offer real time video and control, and have small payload capabilities. Operated within line of sight (LOS) of user.
Group 2 Small Tactical	Weighs 21-55 pounds and normally operates below 3,500 feet AGL at speeds less than 250 knots	Small airframes, low radar cross-sections, and provide medium range and endurance. Requires LOS to the ground control station.
Group 3 Tactical	Weighs more than 55 pounds, but less than 1,320 pounds, and normally operates below 18,000 feet mean sea level (MSL) at speeds less than 250 knots	Range and endurance varies significantly among platforms. Requires a larger logistics footprint than Groups 1 and 2.
Group 4 Persistent	Weighs more than 1,320 pounds and normally operates below 18,000 feet MSL at any speed	Relatively large systems operated at medium to high altitudes. This group has extended range and endurance capabilities (may require runway for launch and recovery)
Group 5 Penetrating	Weighs more than 1,320 pounds and normally operates higher than 18,000 feet MSL at any speed	Operated at medium to high altitudes having the greatest range, endurance, and airspeed. Requires large logistical footprint similar to that of manned aircraft.

D. ORGANIZATION OF THESIS

Chapter II reviews the relevant military doctrine, LSS UAS threat, and C-UAS technologies. Additionally, Chapter II provides a familiarization with the TAK system, previous use, and potential for future development and describes the history and capability

[7] Adapted from Department of the Army, *Counter-Unmanned Aircraft System Techniques*, ATP 3-01.81 (Washington, DC: Department of the Army, 2017), 1-2, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3099_ATP%203-01x81%20FINAL%20WEB.pdf.

of the Dowding C-UAS system. Chapter III documents experiment progress from concept through the final field experimentation with Norwegian Special Operations Forces. Chapter III focuses on the development of the offline Dowding C-UAS system and the TAK's SkyView-Dowding Integration Application (SDIA) which enabled sensor integration. Using the results from Chapter III, Chapter IV analyses the critical factors that SOF team requires to enhance decision making in an enemy UAS-threat environment. Chapter V provides key conclusions as they relate to the research question, reviews the tactical utility of the proposed solution for SOF, and makes recommendations for future research.

II. LITERATURE REVIEW

A. COUNTER UAS PROTECTION: A COMMANDER'S RESPONSIBILITY

The Army's Mission Command philosophy, found in Army Doctrine Publication (ADP) 6-0, outlines the leader's responsibility to employ both the *science of control* and the *art of command* of their assigned units.[8] While the art of command deals with a leader's responsibility to make sound decisions and provide leadership to his soldiers, the science of control includes the establishment and management of systems that improve his understanding and support accomplishing missions.[9] These control systems comprise not only organizational processes and procedures, but the physical networks and information systems that enable the commander to lead. In practice, these systems provide the commander with the situational awareness and communications capabilities to effectively accomplish a given mission.

Though ADP 6-0 extensively discusses a leader's responsibility to command and control his unit to accomplish its mission, the essence of mission command lies in the appropriate delegation of decision-making authority to subordinate leaders.[10] The intent of this philosophy is to provide military leaders with necessary information and flexibility to accomplish their mission. This provides leaders the latitude to seize unexpected opportunities and counter threats inherent to the chaotic nature of military operations. By "empower [ing] subordinate decision making and decentralized execution," mission command philosophy seeks to maximize the effectiveness of military units and facilitate mission accomplishment.[11]

---

[8] Department of the Army, *Mission Command*, ADP 6-0 (Washington, DC: Department of the Army, 2019), 2-1, 3-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN19189_ADP_6-0_FINAL_WEB_v2.pdf.

[9] Department of the Army, 2-1, 3-1.

[10] Department of the Army, 1-5.

[11] Department of the Army, 1-3.

1. Counter-UAS Doctrine

In addition to mission command, Army doctrine requires commanders to protect their troops. Army Doctrine Publication (ADP) 3-37, *Protection*, states that the commander maintains an "inherent responsibility to protect and preserve the force and secure the area of operations (AO) [which] is vital in seizing, retaining, and exploiting the initiative."[12] The commander accomplishes this by following the five Protection Principles: Comprehensive, Integrated, Layered, Redundant, and Enduring.[13] While this concept applies broadly to the protection of U.S. forces writ-large, the Army C-UAS manual, Army Technique Publication (ATP) 3-01.81, addresses the commander's duty to protect U.S. forces through the detection and defeat of LSS drones by tactical level units.[14]

ATP 3-01.81 provides a comprehensive methodology for training, development, and implementation of C-UAS tactics, techniques, and procedures (TTP). In addition to describing planning considerations and techniques for defending against unconventional air threats, the manual emphasizes the importance of integrating sensors and sharing intelligence between echelons.[15] Drawing from the Protection Principles, the doctrine directs the development of integrated sensor, collection, and dissemination plans to establish a common operating picture (COP) for the commander.[16] The sensor plan incorporates available sensors, including radar, acoustic, and radio frequency devices, to provide comprehensive and layered detection, while the collection plan allocates assets to ensure enduring coverage. The dissemination plan also provides leaders with a consistent understanding of their operational environment, allowing them to make appropriate decisions.

---

[12] Department of the Army, *Protection*, ADP 3-37 (Washington, DC: Department of the Army, 2019), 1-3, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18685_ADP%203-37%20FINAL%20WEB_v2.pdf.

[13] Department of the Army, 1-3.

[14] Department of the Army, *Counter-Unmanned Aircraft System Techniques*, 1-1.

[15] Department of the Army, 1-3.

[16] Department of the Army, 1-3.

2. Mission Command and Special Operations

The concept of mission command is especially important in the SOF community and is exemplified in the U.S. Special Operations Command's (USSOCOM) vision statement: "Empowered SOF Professionals, globally networked, partnered and integrated, relentlessly seeking advantage in every domain to compete and win for the Joint Force and the Nation."[17] This concept is further underscored in the Special Operations Forces Operating Concept (SOF-OC), published in 2016.[18] The SOF-OC seeks to improve the future of U.S. SOF by providing an actionable framework that ensures readiness and capabilities of USSOCOM. This document emphasizes the importance of agile and flexible SOF operators and leaders that are empowered to think, act, and operate in complex and uncertain environments as "the risk of not acting, or acting late, can dramatically alter the world landscape, eroding the Nation's security, influence and standing."[19]

The expectations outlined in SOF-OC and USSOCOM's mission statement highlight the need for SOF units to act quickly and without direct oversight, but also without accepting undue risk.[20] This decentralized operational construct and the relative size of SOF units make them difficult to protect. SOF units generally operate with much smaller logistical and defensive footprints than their conventional counterparts and thus rely on specialized training and technological capabilities to enhance their survivability. DoD C-UAS and situational awareness technology must outpace the threats from our enemies, or U.S. SOF operators will continue to be vulnerable in contemporary operating environments.

---

17 "About USSOCOM: Mission Statement and Vision," U.S. Special Operations Command, June 12, 2019, https://www.socom.mil/about.

18 Joseph Votel, *Special Operations Forces Operating Concept: A Whitepaper to Guide Future SOF Development* (Tampa, FL: U.S. Special Operations Command, 2016), https://nsiteam.com/social/wp-content/uploads/2017/01/SOF-Operating-Concept-v1-0_020116-Final.pdf.

19 Votel.

20 U.S. Special Operations Command, "About USSOCOM: Mission Statement and Vision"; Votel, *Special Operations Forces Operating Concept*.

B. CURRENT TECHNOLOGIES

In his 2019 testimony on the posture of U.S. Central Command (CENTCOM), General Joe Votel discussed the importance of technology and organizations like the Joint Improvised Threat Defeat Organization (JIDO) in combatting the most dangerous threats to U.S. forces.[21] Votel specifically commented that CENTCOM relies heavily on critical emerging technologies to counter weaponized UAS that both threaten the safety of U.S. and allied forces and undermine the mission in the area of responsibility.[22] General Tony Thomas, commander of USSOCOM, echoed the importance of technology in his testimony two-weeks later.[23] While General Votel noted the use of technological advances to counter threats, General Thomas' remarks were directed at the use of technology to enable SOF to remain nimble and empower leaders in their execution of mission command. Based on these comments, it is clear that available and emerging technologies in the mission command and C-UAS realm are critical to military success in the contemporary and future operating environments.

1. Mission Command Technology and the Tactical Assault Kit

The Tactical Assault Kit (TAK) is a family of tools used on Android, Windows, and web-based systems.[24] Special Operations Forces primarily employ the Android TAK (ATAK), an Android phone-based end user device (EUD) which provides a common operating picture using overlaid Global Positioning System (GPS) information and National Geospatial-Intelligence Agency (NGA) map data.[25] TAK uses an intuitive graphic user interface (GUI) to allow its users to quickly and simply operate various tools to enhance situational awareness and accomplish specific tasks. The flexibility of the TAK

---

[21] *Posture Statement of the U.S. Central Command and the Current and Future Challenges in the Middle East: Testimony before the Senate Armed Services Committee*, 116th Cong. (2019) (statement of Joseph Votel, Commander, U.S. Central Command).

[22] Votel, testimony on *U.S. Central Command and the Current and Future Challenges*.

[23] *Posture Statement of the U.S. Special Operations Command: Testimony before the Senate Armed Services Committee*, 116th Cong. (2019) (statement of Raymond Thomas, Commander, U.S. Special Operations Command).

[24] "What is TAK?," Tactical Assault Kit, accessed February 7, 2019. https://takmaps.com.

[25] Tactical Assault Kit.

system gives users the capability to create and upload applications and plug-ins that perform general functions such as identifying the locations of other TAK users, and task-specific functions like military freefall planning suites, counter weapons of mass destruction sensors, and precision runway survey tools. Most importantly, the TAK platform brings together these disparate planning and situational awareness functions on a single device, while enabling all connected users to share a COP.

The TAK system allows users to share information, like the locations of friendly or enemy elements, by passing cursor-on-target (CoT) data between devices. CoT data is data protocol designed to allow tactical systems to quickly communicate critical information between devices and is the primary language used by the TAK.[26] Users pass this message traffic by pairing TAK enabled devices to specifically designed mesh network radio nodes, such as the Persistent System Wave Relay radios, or by connecting devices to a central computer processor specifically designed to route CoT data messages called a TAK Server.[27]

While the Android-specific ATAK is the most commonly used configuration of the TAK system, the program is also designed to work on Windows (WinTAK), in a Virtual Reality planner (VTAK), and a government civilian version (TAK-Civ). Additionally, recent research conducted at the Naval Postgraduate School led to the development of the Joint Operations Center TAK (JOCTAK).[28] Recognizing the inability of an Android-based platform to provide adequate processing power and display outputs for an operations center, the JOCTAK construct sought to bring the tactical utility and flexibility of the ATAK system to the operational headquarters.[29] By creating an operational-level system that integrates directly with the proven ATAK system, the developers effectively bridged

---

[26] Michael J. Kristan et al., *Cursor-on-Target Message Router User's Guide*, Report Number MP090284 (Bedford, MA: MITRE Corporation, 2009), 2-1, https://doi.org/10.21236/ADA640597.

[27] "MPU5: The World's First Smart Radio," Persistent Systems, 2017, https://www.persistentsystems.com/site/wp-content/themes/persistensystems/pdf/mpu5/mpu5_spec_sheet.pdf; Tactical Assault Kit, "What is the TAK?"

[28] Daniel Bandy et al., "JOKTAK: Joint Operations Center Tactical Assault Kit" (Defense Analysis poster, Naval Postgraduate School, 2018), http://hdl.handle.net/10945/58015.

[29] Bandy et al., 4.

the information and situational awareness gaps between decentralized ground units and their command headquarters.

The TAK's flexibility and functionality allow commanders and operators to communicate provided that users are networked. The TAK is not restricted to a standardized network configuration and operates across both open and closed networks. Acknowledging that capability, certain network configurations are preferred for specific mission sets. Radio advancement, especially software defined radio technologies, provides users the ability to communicate larger volumes of data in addition to voice transmissions.[30] This increase in communications capability allows users to send and receive data streams while conducting decentralized operations. The TAK, operating over a wireless communication network, meets the operator's demand for consistent connectivity between teams and higher headquarters.

Two types of wireless communication networks exist: infrastructure-based and ad hoc.[31] Figure 2 depicts the differences between infrastructure-based and ad hoc networks. Infrastructure-based networks use centralized hardware to connect wireless networks, through a wireless access point (WAP), to wired networks, through a switch.[32] Users operating on infrastructure-based networks are reliant on the WAP and switch to access data residing on wired networks. A mobile ad hoc network (MANET) is a "peer-to-peer, multihop connected network [that] is composed usually of tens to hundreds of mobile nodes."[33] A MANET is "used to connect wireless clients directly together, without the need for a wireless access point or a connection to an existing wired network."[34] In a MANET, "each individual node must be able to act both as a host, which generates user

---

[30] Jon Harper, "Military, Industry Gung-Ho on Software Defined Radios," *National Defense*, February 15, 2019, https://www.nationaldefensemagazine.org/articles/2019/2/15/military-industry-gung-ho-on-software-defined-radios.

[31] Jonathan Loo, Jaime Lloret Mauri, and Jesus Hamilton Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends* (Boca Raton, Florida: CRC Press, 2012), 4.

[32] Loo, Mauri, and Ortiz, 4.

[33] Doina Bein, "Self-Configuring, Self-Organizing, and Self-Healing Schemes in Mobile Ad Hoc Networks," in *Guide to Wireless Ad Hoc Networks*, ed. Sudip Misra, Isaac Woungang, and Subhas Misra (London: Springer Science and Business Media, 2009), 27.

[34] Loo, Mauri, and Ortiz, *Mobile Ad Hoc Networks*, 4.

and application traffic, and as a router."[35] In a military application, the primary advantage of the MANET is the ability for hosts to "remain connected while they are moving around" by freeing users from a central WAP, which facilitate inter-team communication even if connectivity is lost with higher headquarters.[36] When infrastructure-based and MANETs are linked together, decentralized teams and higher headquarters form larger, more resilient networks. Combining the advantages of wireless and wired networks, commanders have access to the full suite of TAK infrastructure capabilities.

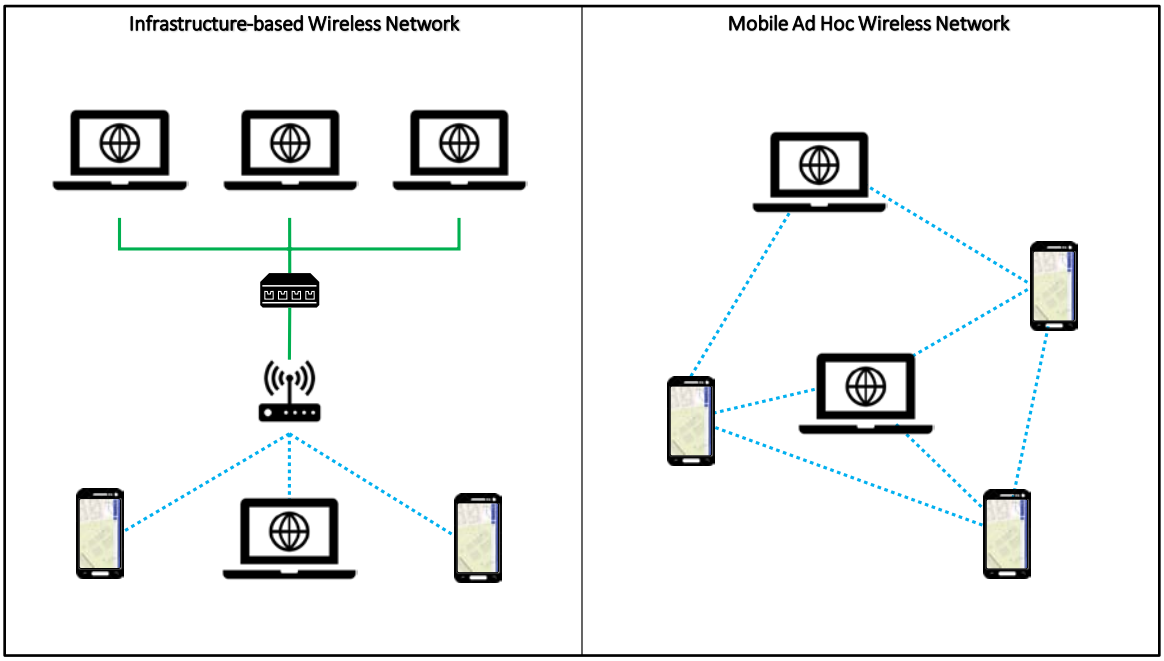


Figure 2. Infrastructure and Mobile Ad Hoc Wireless Networks

Most importantly, ATAK facilitates the mission command concept of delegated authority. In a qualitative leap beyond traditional radio communication technologies, ATAK empowers subordinate commanders with near real-time situational awareness. This

[35] Doina Bein, "Self-Configuring, Self-Organizing, and Self-Healing Schemes in Mobile Ad Hoc Networks," 27.

[36] Loo, Mauri, and Ortiz, *Mobile Ad Hoc Networks*, 5.

vast improvement in understanding and awareness allows leaders at all levels to make faster, more informed decisions.

2. Current Uses

Prior TAK-focused research and development projects addressed various capability gaps including the lack of integrated mission planning tools, the policy preventing SOF teams from physically accompanying host nation partners, the creation of an operational level TAK system, and the integration of sensors to detect Chemical, Biological, Radiological, Nuclear (CBRN) threats and countering weapons of mass destruction (CWMD). These projects evolved from the Remote Advise and Assist (RAA) kit into the Advanced Digital Adviser Partnering Technologies (ADAPT) which created the Collaborative Mission Planner (CMP) and later branched into the JOCTAK.[37] The RAA kit connects Special Forces advisors to their partner forces through the integration of multiple technologies including geospatial software and satellite communication hardware.[38] As seen in Figure 3, the CMP integrates mission planning features into the TAK to better share understanding and remove the requirement to build separate planning products.[39] The JOCTAK system unifies all TAK systems and provides a common operational picture to each user by amalgamating and redistributing information.[40] The JOCTAK system uses the RAA concept to integrate CBRN sensors to allow commanders to more rapidly adjudicate fissile material detection and identification, and enables them to efficiently allocate resources while conducting the CWMD mission.[41] As USSOCOM's choice tool to support mission command, the TAK allows for the integration of emerging technologies within a flexible software application.

---

[37] Bandy et al., "Joint Operations Center Tactical Assault Kit (JOCTAK)," 27-28.

[38] Christopher Thielenhaus and Eric Roles, "Maximizing the Utility of Special Warfare: The Remote Advise and Assist Concept" (master's thesis, Naval Postgraduate School, 2016), 53-54.

[39] Michael Ferriter, Phil Schupp, and Sverre Wetteland, "Organizing Chaos: The Tactical Assault Kit Collaborative Mission Planner" (master's thesis, Naval Postgraduate School, 2017), 16, http://hdl.handle.net/10945/56915.

[40] Bandy et al., "Joint Operations Center Tactical Assault Kit (JOCTAK)," 4.

[41] Bandy et al., 4-5.

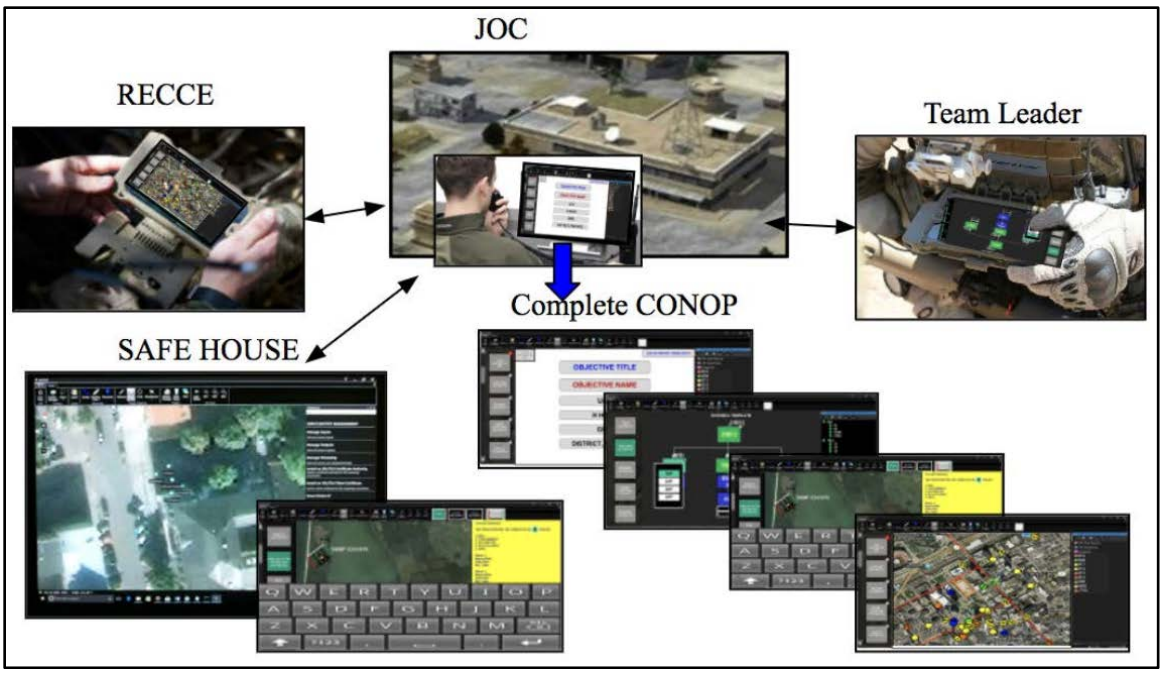


Figure 3. TAK Collaborative Mission Planner Concept[42]

3. Threat UAS Technologies

To counter their inferior resources and technological capabilities, militant groups have long pursued innovative methods to inflict harm on state militaries. In the contemporary operating environment, groups such as ISIS, Al-Qaeda, and the Taliban have consistently used unconventional tactics like suicide bombers and improvised explosive devices (IED), to seek parity in their unbalanced war against the United States and the West. As the U.S. military adapted to these TTPs, these tactics became less effective against military forces, driving militants to expand their search for an inexpensive weapon capable of harming U.S. forces; they found their weapon in COTS LSS UAS.[43]

While the use of UAS by non-state actors is not necessarily a new concept—Hamas has used Iran-provided drones since at least 2004—the proliferation of commercial-use

[42] Ferriter, Schupp, and Wetteland, "Organizing Chaos," 16.

[43] Don Rassler, "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology," Combating Terrorism Center at West Point, October 20, 2016, 11, https://ctc.usma.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology.

drones presents a novel threat.[44] Violent extremist organizations (VEO), use numerous types of LSS UAS including commercially available multi-copters, larger fixed-wing platforms, and even completely homemade aircraft.[45] These organizations use their UAS predominantly in three ways: as a reconnaissance and surveillance asset, as a fires platform, and to film attacks for propaganda purposes.[46]

The Islamic State's drone program was first reported in August 2014.[47] Though initially used merely to generate propaganda and provide situational awareness to leaders, ISIS began weaponizing commercial drones by summer 2016.[48] While the earliest models of armed drones were nothing more than unmanned vehicle-borne improvised explosive devices (VBIED), by December 2016, ISIS drones were capable of dropping grenade-sized munitions on unsuspecting soldiers and bases with relative precision.[49] While aerial fires are currently the predominant threat posed to U.S. forces by SUAS, technological advances may prove to be far more dangerous.

Though the current UAS threat is real, emerging threats of autonomous swarm technology and aerial dispersion of chemical and biological agents are potentially the most

---

[44] Alyssa Sims, "The Rising Drone Threat from Terrorists," *Georgetown Journal of International Affairs* 19, no. 1 (2018): 97-107, https://doi.org/10.1353/gia.2018.0012.

[45] Dan Gettinger, "Drones Operating in Syria and Iraq" *Center for the Study of the Drone at Bard College* (blog), December 2016, 1-2, https://dronecenter.bard.edu/files/2016/12/Drones-in-Iraq-and-Syria-CSD.pdf.

[46] Asaad Almohammad and Anne Speckhard, "ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics," *International Center for the Study of Violent Extremism* (blog), May 2017, 2-3, http://www.icsve.org/research-reports/isis-drones-evolution-leadership-bases-operations-and-logistics.

[47] Yasmin Tadjdeh, "Islamic State Militants in Syria Now Have Drone Capabilities," *National Defense*, August 28, 2014, https://www.nationaldefensemagazine.org/articles/2014/8/28/islamic-state-militants-in-syria-now-have-drone-capabilities.

[48] Almohammad and Speckhard, "ISIS Drones," 2-3.

[49] Steven Stalinsky and R. Sosnow, "A Decade of Jihadi Organizations' Use of Drones - From Early Experiments by Hizbullah, Hamas, and Al-Qaeda to Emerging National Security Crisis for the West as ISIS Launches First Attack Drones," *Middle East Media Research Institute,* Inquiry and Analysis 1300 (February 21, 2017), https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda.

concerning future threat for the U.S. military.[50] Using commercially available technology meant for crop-spraying, VEOs can develop mobile, dispersal platforms for chemical and biological weapons.[51] The use of chemical weapons is already a prevalent threat in Syria, with over 300 confirmed uses during the Syrian Civil War (2012-2018).[52] The potential for SUAS to be used as a method of dispersion only exacerbates this threat to American forces in the region. While the use of this tactic has not been reported, this technology is widely available and VEOs could easily employ this capability.

While not currently as technologically obtainable as aerial dispersion, autonomous swarm technology has the greatest potential to devastate the current U.S. drone defenses. Autonomous swarms are networked groups of unmanned systems programmed to accomplish specific tasks without human input.[53] When this technology is applied to SUAS, the drones are capable of identifying targets, conducting precision attacks, intelligently defeating countermeasures, and overwhelming air defense systems.[54] Because of their autonomous nature, groups of intelligent swarms can also be used to conduct extremely complex attacks without endangering the operator or other militants on the ground.

While the threat of militant UAS use is consistently changing, Don Rassler from the Combatting Terrorism Center at West Point sums up the current state of the threat perfectly:

---

[50] Irving Lachow, "The Upside and Downside of Swarming Drones," *Bulletin of the Atomic Scientists* 73, no. 2 (2017): 96-98, https://doi.org/10.1080/00963402.2017.1290879; Ahmet S. Yayla and Anne Speckhard, "The Potential Threats Posed by ISIS's Use of Weaponized Air Drones and How to Fight Back," *International Center for the Study of Violent Extremism* (blog), March 1, 2017, https://www.icsve.org/the-potential-threats-posed-by-isiss-use-of-weaponized-air-drones-and-how-to-fight-back.

[51] Yayla and Speckhard, "The Potential Threats Posed by ISIS's Use of Weaponized Air Drones and How to Fight Back."

[52] Tobias Schneider and Theresa Lutkefend, "Nowhere to Hide: The Logic of Chemical Weapon Use in Syria," *Global Public Policy Institute Study* (blog), February 2019, https://www.gppi.net/media/GPPi_Schneider_Luetkefend_2019_Nowhere_to_Hide_Web.pdf.

[53] M. Rubenstein, C. Ahler, and R. Nagpal, "Kilobot: A Low Cost Scalable Robot System for Collective Behaviors," in *IEEE International Conference on Robotics and Automation* (2012), 3293-98, https://doi.org/10.1109/ICRA.2012.6224638.

[54] Don Rassler, "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology," 50-54.

> Currently, the use of a single UAS by terrorists piloted by remote control remains a "niche" threat and is best understood as being a moderate probability, and low-to-moderate threat in terms of lethality. While the use of a group of drones, or an autonomous swarm, by terrorist entities has not yet been observed, the use of more and more sophisticated drones is likely to enhance the scope and seriousness of the threat, and affect the consequence of future incidents.[55]

4. C-UAS Technologies

SOF units require C-UAS capabilities that are as versatile and agile as their own formations. As such, they require detection capabilities that are portable, require little power, and can be maintained in austere environments.

Counter-UAS (C-UAS) technology generally falls into one of two categories: detection and interdiction. The current detection mechanisms predominantly use one or more of three sensor technologies to identify and track UAS: acoustic, radio frequency (RF), and radar.[56] In the UAS detection realm, no single sensor, or even sensor type, is the panacea; when considering their size, cost, and effectiveness, each has a distinct weakness.[57] Table 2 depicts the advantages and disadvantages of acoustic, RF, and radar C-UAS sensors. While the strengths and weaknesses of sensors vary across the spectrum of technologies, one weakness remains consistent: they have not been appropriately integrated with situational awareness tools, and most do not communicate with each other.

---

[55] Rassler, 63

[56] J.R. Wilson, "The New World of Counter-Drone Technology," *Military and Aerospace Electronics*, November 1, 2018, https://www.militaryaerospace.com/articles/print/volume-29/issue-11/special-report/the-new-world-of-counter-drone-technology.html.

[57] Wilson.

Table 2. Advantages and Disadvantages of C-UAS Sensor Types[58]

Type of Sensor	Advantages	Disadvantages
Acoustic	Sound emission detection Size and weight Omnidirectional Night/day	Range Weather Environmental noise Ruggedization
Radio Frequency	Target Ground Control Station Ability to classify target Size and weight Dismounted portability Range Weather Ruggedization Omnidirectional Night/day	Drone waypoint mode Requires load set
Radar	Weather Range Ruggedization Omnidirectional Night/day	Cost Ability to classify target Power consumption Size and weight Detection angle

a. Acoustic Detection

As the name suggests, acoustic detection devices listen for the sounds produced by the rotors or engine of an UAS. Specifically, "acoustic sensing is a passive technology that involves the detection of acoustic wave energy produced by some oscillating body."[59] Microphones "detect pressure fluctuations created during wave transmission" and are designed for omnidirectional detection.[60] Sensors capable of omnidirectional detection of faint noises have their obvious benefits when compared against other types of C-UAS sensors.

---

[58] Adapted from Sai Ram Ganti and Yoohwan Kim, "Implementation of Detection and Tracking Mechanism for Small UAS," in *International Conference on Unmanned Aircraft Systems* (2016), https://doi.org/10.1109/ICUAS.2016.7502513; Ismail Guvenc et al., "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," in *IEEE/AIAA 36th Digital Avionics Systems Conference* (September 2017), 6, https://doi.org/10.1109/DASC.2017.8102043; P. Poitevin, M. Pelletier, and P. Lamontagne, "Challenges in Detecting UAS with Radar," in *International Carnahan Conference on Security Technology* (2017), 1, https://doi.org/10.1109/CCST.2017.8167852; "Giraffe 1X Short Range 3D Radar," Saab Solutions, accessed June 18, 2019, https://saab.com/air/sensor-systems/ground-based-air-defence/giraffe-1x.

[59] Brendan Harvey and Siu O'Young, "Acoustic Detection of a Fixed-Wing UAV," *Drones* 2, no. 1 (2018): 1, https://doi.org/10.3390/drones2010004.

[60] Harvey and O'Young, 1.

Microphones can also be built from micro-electromechanical systems (MEMS). MEMS are "structures or mechanisms with one or more geometrical dimension on the order of one to hundreds of micrometers in size and comprise small electro-mechanical systems that are produced utilizing microfabrication techniques."[61] MEMS technology is not specific to acoustic sensors or defense applications and can be used across a broad spectrum of disciplines ranging from biology to inertial sensing.[62] MEMS acoustic sensors provide the added benefit of being both small and lightweight which reduce the dismounted operator's weight and power requirements. However, MEMS acoustic sensors are difficult to ruggedize and are adversely affected by weather, moisture, and dust.[63]

Researchers and students at the Naval Postgraduate School's Consortium for Robotics and Unmanned Systems Education and Research (CRUSER) are developing MEMS acoustic sensors directed at collecting and studying UAS acoustic signatures.[64] The research effort is based on the replication of the mechanically coupled ears of the *Ormia ochracea* fly in a narrowband MEMS direction finding sensor.[65] Still in the development phase, the MEMS acoustic directional sensors use spectral characteristics to detect motion with a single sensor.[66] The goal for the MEMS acoustic directional sensors is to remove ambient sound clutter and have the capability to be tuned to detect specific UAS harmonics.[67]

---

61 Daniel Hogue and Sarah Gregory, "MEMS-Based Waste Vibrational Energy Harvesters" (master's thesis, Naval Postgraduate School, 2013), 3. https://calhoun.nps.edu/handle/10945/34678.

62 "MEMS and Nanotechnology Applications." MEMS Exchange, accessed February 8, 2019. https://www.mems-exchange.org/MEMS/applications.html.

63 Squarehead Technology, "Squarehead Unveils Discovair G2," *Squarehead News* (blog), August 3, 2018, https://www.sqhead.com/squarehead-unveils-discovair-g2.

64 Fabio Alves and Gamani Karunasiri, "MEMS Acoustic Directional Finder for Small Flying UAS" (CRUSER's TechCon, Naval Postgraduate School, 2018), https://calhoun.nps.edu/handle/10945/58040.

65 Daniel Wilmott, Fabio Alves, and Gamani Karunasiri, "Bio-Inspired Miniature Directional Finding Acoustic Sensor," *Nature Scientific Reports* 6, 29957 (2016), 1. https://www.nature.com/articles/srep29957.

66 Fabio Alves and Gamani Karunasiri, "MEMS Acoustic Directional Finder for Small Flying UAS."

67 Todd Coursey, "MEMS Acoustic Sensor for Drone Detection" (presentation, Naval Postgraduate School, Monterey, CA, April 11, 2017), https://calhoun.nps.edu/handle/10945/53349.

Acoustic sensors are limited by the existence of wind and environmental noise which clutters the sensors' ability to detect unique sounds from the UAS.[68] Environmental noises range from persistent city noise to battlefield sounds such as gunfire and artillery. The effects can overwhelm the acoustic sensors and make them ineffective. An industry-leading example of an acoustic C-UAS sensor is the Discovair G2 developed by the Norwegian company, Squarehead Technologies. Squarehead has developed a ruggedized acoustic sensor consisting of 128 MEMS microphones capable of detecting and tracking UAS in an effort to make acoustic C-UAS sensors viable.[69] The Discovair G2 was built specifically to operate in austere environments and was purposely built with a robust application program interface (API) for integration with situational awareness tools.[70] Figure 4 shows a scientist from Squarehead operating the Discovair G2 with the authors in Norway.

Figure 4. Squarehead Discovair G2

68 G. J. Mendis et al., "Deep Learning Based Doppler Radar for Micro UAS Detection and Classification," in *IEEE Military Communications Conference* (2016), 1, https://doi.org/10.1109/MILCOM.2016.7795448.

69 "Discovair: Acoustic Drone Detection," Squarehead Technology, October 2018, https://www.sqhead.com/wp-content/uploads/2018/10/Drone-Detection-Discovair-G2-brochure.pdf.

70 Squarehead Technology, "Discovair: Acoustic Drone Detection."

b. Radio Frequency Detection

Radio Frequency sensor technologies provide a dependable, long-range C-UAS detection capability.[71] The SUAS and the associated ground control station (GCS) communicate with each other through radio wave transmissions. Generally, SUAS use Wi-Fi, transmitted over 2.4 gigahertz Ultra High Frequency (UHF) waves, to communicate between the airframe and the GCS.[72] A GCS can use a flight controller, smartphone, or tablet to communicate with the SUAS via Wi-Fi.[73] Radio frequencies also transmit between onboard cameras or other payloads to the GCS.[74] These frequency emissions can be exploited by RF sensor technology and used to locate the SUAS and GCS. Another advantage of RF sensors is their size and weight which allows for dismounted and mounted configurations, as depicted in Figure 5.

Radio frequency C-UAS technology broadly applies to the sensing, detecting, and jamming of devices, and is sub-divided into passive and active collection. Passive collection sensors detect signals transmitted between the SUAS and the GCS while active sensors emit radio frequencies which reflect off the SUAS and return to the receiver.[75] Although passive RF collection is dependable, it is not without limitations. SUAS flying to preset waypoints do not necessarily transmit signals back to the ground control station when flying autonomously. The waypoint mode technology allows enemy SUAS operators to preprogram missions into the SUAS before launching, which allows operation without an RF signature.[76] Another weakness of passive collection is the requirement for RF-based C-UAS sensor operators to maintain an updated load set for the various frequencies that each unique SUAS transmits. A

---

71 Ganti and Kim, "Implementation of Detection and Tracking Mechanism for Small UAS," 1255.

72 John Patrick Pullen, "This Is How Drones Work," *Time*, April 3, 2015, https://time.com/3769831/this-is-how-drones-work.

73 Pullen.

74 Guvenc et al., "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," 6.

75 Phuc Nguyen et al., "Investigating Cost-Effective RF-Based Detection of Drones," in *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use* (2016), 18, https://doi.org/10.1145/2935620.2935632.

76 H. Fu et al., "Low-Complexity Portable Passive Drone Surveillance via SDR-Based Signal Processing," *IEEE Communications Magazine* 56, no. 4 (April 2018), 115, https://doi.org/10.1109/MCOM.2018.1700424.

load set is a library of frequencies the SUAS and GCS transmit, which must be programmed into the RF sensor for the C-UAS device to properly detect, catalogue, and jam. Personnel with ground experience in Afghanistan, Iraq, and Syria will recognize this process as being similar to the load sets filled into the Counter Remote Controlled Improvised Explosive Device Electronic Warfare (CREW) systems. If the correct load set is not filled into the C-UAS sensor, neither the aircraft nor the GCS can be detected.

Figure 5. SkyView RF Sensor in Dismounted and Vessel Mounted Configurations

c. Radar

Unlike RF, which detects signals being sent between an aircraft and its GCS, radar detects the target itself. Radar stands for Radio Detection and Ranging, and in simplified terms, radar detects targets by sending out a pulse which reflects off a target's cross-section and returns back through propagation.[77] This process results in five primary radar

[77] Robert O'Donnell, *RES.LL-001 Introduction to Radar Systems* (Massachusetts Institute of Technology: MIT OpenCourseWare, 2007), https://ocw.mit.edu/resources/res-ll-001-introduction-to-radar-systems-spring-2007.

observables: target range, target angles (including azimuth and elevation), target size (also known as radar cross-section), target speed, and target features.[78] Using the Doppler effect, radar can distinguish between moving and static objects and determine speed.[79] Speed data, combined with range and angle measurements, allow the radar to locate targets.

In 2015, radar research, focused on the detection and classification of LSS UAS, barely existed.[80] However, in the few years since ISIS began using LSS UAS on the battlefield, the demand for layered C-UAS detection systems spurred the scientific community to make significant developments using radar. The benefits of radar detection include ranged detection of moving or static objects, all-weather capability, night and day use, and 360-degree coverage.[81] The disadvantages of radar include the difficulties associated with detection of targets with small radar cross-section (RCS), low speeds, and low altitudes.[82] A major gap currently being overcome is the inability for radar systems to classify and discriminate between detections. To target LSS UAS, a radar's detection threshold must decrease which also results in the detection of birds and other small flying objects.[83] Despite this limitation, radar's shown potential for detecting UAS combined with the increased UAS threat has driven radar producers to optimize radars specifically for UAS detection.

Tradeoffs exist between the intended purpose of a radar, its cost, physical size, and alternative utilizations.[84] For example, a radar whose primary purpose is to detect next generation fighter jets is optimized for that purpose. Although that system will be able to detect Group 4 and 5 UAS, it will perform poorly against LSS UAS due to optimization considerations such as algorithms used, frequencies, and bandwidth. Rotating radars provide 360-degree coverage, a crucial element for detecting enemy LSS UAS deployed from any

---

[78] O'Donnell.

[79] O'Donnell.

[80] Francesco Fioranelli et al., "Classification of Loaded/Unloaded Micro-Drones Using Multistatic Radar," *Electronics Letters* 51, no. 22 (2015): 1813-15, https://doi.org/10.1049/el.2015.3038.

[81] Poitevin, Pelletier, and Lamontagne, "Challenges in Detecting UAS with Radar," 1.

[82] Guvenc et al., "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," 2.

[83] Ganti and Kim, "Implementation of Detection and Tracking Mechanism for Small UAS," 1255.

[84] Poitevin, Pelletier, and Lamontagne, "Challenges in Detecting UAS with Radar," 2-3.

direction. Radar's advantages make it an important sensor in layered C-UAS detection; however, the LSS UAS poses a unique challenge which requires an adaptation away from conventional radar use.

The inherent characteristics of LSS UAS challenge conventional radar systems due to the low altitude flight, slow speeds, and small RCS.[85] Although radars conduct 360-degree detection, radar is limited to a range of elevation coverage.[86] The idiom "flying under the radar" absolutely applies to LSS UAS as a radar gauged for a high-altitude threat will be unable to detect low flying UAS. Ground moving-target indication (GMTI) radars use specific target speed thresholds, called Minimum Detectable Velocity (MDV), to allow the sensor to distinguish the target from the ground.[87] The low speeds of LSS UAS are inseparable from clutter, and the LSS UAS evades detection.[88] To detect LSS UAS by radar, the Signal to Noise Ratio (SNR) must reach a point where the radar detects a weak signal and distinguishes it from surrounding noise.[89] The minimal radar cross-section produced by LSS UAS complicates detection as the small target does not allow for radar signals to reflect back towards the radar receiver.[90] To mitigate the challenges of a small RCS, higher frequency radars can be used, as the cross-section is proportional to frequency.[91]

Principal C-UAS detection research and testing has focused on a wide array of radar technologies to address the low RCS issue. In 2018, researchers at the Universidad Politécnica de Madrid devised an X-band frequency modulated continuous wave (FMCW) radar to detect a DJI Phantom-4 drone at a range up to two kilometers.[92] Research by Guvenc et al., from 2017 points to the viability of Extremely High Frequency (EHF) mmWave radar drone

---

85 Fioranelli et al., "Classification of Loaded/Unloaded Micro-Drones Using Multistatic Radar," 1.

86 Poitevin, Pelletier, and Lamontagne, "Challenges in Detecting UAS with Radar," 1.

87 John Alfred Richards, *GMTI Radar Minimum Detectable Velocity*, Report Number SAND2011-1786 (Albuquerque, NM: Sandia National Laboratories, 2011), 3, https://doi.org/10.2172/1011708.

88 Richards, 3.

89 Poitevin, Pelletier, and Lamontagne, "Challenges in Detecting UAS with Radar," 2.

90 Poitevin, Pelletier, and Lamontagne, 2.

91 Poitevin, Pelletier, and Lamontagne, 2.

92 Á D. de Quevedo et al., "Drone Detection with X-Band Ubiquitous Radar," in *19th International Radar Symposium* (2018), 1-3, https://doi.org/10.23919/IRS.2018.8447942.

detection.[93] Using mmWave radar, Guvenc detected a DJI Phantom 2 and a DJI S1000 at ranges between 30 to 90 meters.[94] Three-dimensional (3D) X-band radar, like Saab's Giraffe 1X, provides 360-degree coverage and the capability to identify drone elevation in a package capable of mounting on a light vehicle.[95] Even the most compact radars, such as the Giraffe 1X seen in Figure 6, weigh over 600 lbs, which prevents dismounted forces from employing the radar. At this time, the size and the weight of radar does not provide enough of a reasonable advantage to change doctrine, equipment, and TTPs when compared against the LSS UAS threat.

Figure 6. Saab Giraffe 1X Radar[96]

The literature points to radar's challenges with classification and discrimination of target type but also to opportunities.[97] While technical issues persist, the professional debate

[93] Guvenc et al., "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," 2-3.

[94] Guvenc et al., 2-3.

[95] Saab Solutions, "Giraffe 1X Short Range 3D Radar."

[96] Source: Saab Solutions, "Giraffe 1X Short Range 3D Radar."

[97] Guvenc et al., "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," 2, 5; Poitevin, Pelletier, and Lamontagne, "Challenges in Detecting UAS with Radar," 1-4; Quevedo et al., "Drone Detection with X-Band Ubiquitous Radar," 1.

also highlights the significant developments made in radar technology since 2015. Another issue not discussed in the literature is the size and weight disadvantage. For base defense, the 3D radar solution could immediately be used at remote SOF bases. For SOF employment, systems like the Giraffe 1X can mount on the Ground Mobility Vehicles (GMV) or on SOF non-tactical vehicles (NTV); however, commanders must account for the size to weight ratio and its physical signature. Although radar continues to be miniaturized and man-packable systems exist, the current systems optimized for LSS UAS detection are not man-packable.

C. C-UAS SENSOR INTEGRATION AND TAK

The integration of UAS detection devices with situational awareness tools such as the TAK could enhance survivability for troops on the ground through improved detection and fusion targeting enemy SUAS. A SUAS sensor, connected using either a specialized TAK Server or MANET designed for CoT transport, would provide location information to all networked devices.

At this point, most sensor to ATAK integration is left to the sensor companies, rather than at the central ATAK program office. Often these plug-ins are developed on a single version of the ATAK firmware and, as such, many vendor-based plug-ins are not compatible with all versions of ATAK.[98] This presents a significant problem when trying to use multiple sensors on the same ATAK network.

To solve this problem, several organizations, including the Asymmetric Warfare Group (AWG), Defense Innovation Unit (DIU), and the Army Combat Capabilities Develop Command (CCDC), have developed solutions to mass-integrate disparate sensors. Each of these organizations uses a different approach to solving the problem, and each system has distinct strengths and weaknesses.

[98] Charlie Johnson and Brandon Dodd, personal communication, April 30, 2019.

1. Asymmetric Warfare Group's Defense-in-Depth Exercise

In November 2018, AWG conducted a large-scale experiment to test 15 unique counter-UAS devices and to integrate them into the TAK environment.[99] Because many of the sensors did not have a functioning ATAK plug-in, the experimenters used ingest protocols in a TAK server to create CoT data to distribute to the ATAK devices. Because this solution used unspecific protocols, the server would often produce a CoT for identified false positives. As a result, ATAK users were often overwhelmed with a COP containing icons that were either not UAS (false positives) or multiple icons for the same UAS threat (redundant reporting).[100] By maximizing the number of C-UAS technologies, the experiment sacrificed precision; this issue is an important factor that has not been solved and critical for future research to explore.

The AWG conducted Defense-in-Depth Exercise (DiDEX) 2018 at Fort A.P. Hill, VA in November 2018 and brought together multiple C-UAS system vendors and conventional Army forces to explore "best practices for employing multiple C-UAS capabilities against a LSS UAS threat."[101] The DiDEX experiments arrayed the 15 C-UAS technologies in depth and employed conventional forces at a Battalion Command and Control (C2) node, Company C2 node, and in mobile elements.[102] While DiDEX included both the detect and defeat capabilities of the C-UAS construct, it was not scoped to focus on the nuanced requirements of detecting, tracking, and classifying SUAS or how to best present this data using SA tools. Additionally, the experiment did not account for the specific needs of a dismounted SOF team operating in a decentralized environment.

---

99 Asymmetric Warfare Group, *Defense-in-Depth Experiment (DiDEX) 2018 Final Report* (Fort A.P. Hill, VA: Asymmetric Warfare Group, 2019), 6.

100 Asymmetric Warfare Group, *Defense-in-Depth Experiment (DIDEX) 2018 Observation Report*, (Fort A.P. Hill, VA: Asymmetric Warfare Group, 2019), 6-8.

101 Asymmetric Warfare Group, *DiDEX 2018 Final Report*, 8.

102 Asymmetric Warfare Group, 6, 14.

2. Army Combat Capabilities Development Command's FOCUS

The Army CCDC solution to C-UAS sensor integration is the in-development, vehicle-based integration system FOCUS. The FOCUS system uses a Sensor Interface Module (SIM) that ingests specific sensor feeds using a TAK server.[103] Unlike the TAK server used in the DiDEX experiment, the FOCUS system has optimized protocols and fusion algorithms for six specific sensors in order to maximize the efficiency of the system. This framework sacrifices broad applicability for precision and accuracy.

The sensors identified for FOCUS integration are the L3 Coppola Light (EO/IR), Squarehead Discovair G2 (acoustic), Verus SkyView (RF), U.S. Army Darkbridge (RF), AFRL Ninja (RF), and the SkySafe MM2 (RF).[104] By integrating only specific sensors and incorporating a fusion algorithm, FOCUS can effectively relay information to the warfighter, without inundating the COP with extraneous or inaccurate information.

The limitations of the FOCUS system are its form-factor and the limited number of compatible sensors. In its current state of development, CCDC's system is designed for a general purpose force and optimized to be mounted into a vehicle due to its size and power requirements. As such, it is not an optimal tool for SOF units operating without a vehicular mobility capability. The system is also limited by the integrated sensors. While limiting the number of sensors allows SIM to function more efficiently, it also excludes potential detection capabilities, like radar (entirely) and other capable RF, EO/IR, and acoustic sensors.

3. Defense Innovation Unit's Dowding C-UAS System

Another unique approach to UAS sensor integration is DIU's server-based "Dowding C-UAS."[105] DIU named its project after the Dowding System, an air defense network developed during the Battle of Britain and named for Fighter Command's Commander-in-Chief, Air Chief Marshal Sir Hugh Dowding.[106] The World War 2 era Dowding System

---

[103] Brandon Dodd, personal communication, April 30, 2019.

[104] Brandon Dodd, personal communication, April 30, 2019.

[105] Ryan Beall, *Windtalker Overview* (Mountain View, CA: Defense Innovation Unit, 2019).

[106] "What Was The 'Dowding System'?," Imperial War Museums, last modified June 18, 2018, http://www.iwm.org.uk/history/what-was-the-dowding-system.

"brought together technology, ground defenses and fighter aircraft into a unified system of defence" which "not only controlled the fighter force, but other elements…including anti-aircraft guns, searchlights, and barrage balloons."[107] This full integration of humans, organizations, sensors, and shooters inspired DIU's vision for the C-UAS tool.

The Dowding C-UAS server uses government-open source software as a platform to ingest sensor data and exports CoT data to various situational awareness platforms. In this way, the Dowding Server functions much like a highly specialized, custom TAK server. In addition to a web user interface (UI), Dowding also pushes data to an Android-based UI and a developing ATAK plug-in. While the system does not currently work with all sensors, the modular nature of the software allows the DIU, or other users with access, to quickly add protocols to ingest specific sensor data. Unlike a typical ATAK plug-in, Dowding software is constantly monitored for version compatibility each time it is updated. This allows Dowding to run on different versions of ATAK without issue.

Unlike other current solutions which are primarily designed around a single hardware solution, the Dowding system was also designed to work on multiple platforms to allow a variety of applications of the same software. Because of this modular design, Dowding can be run on a server, a computer, or even from a data cloud.

The main drawback to the Dowding Server is its optimization for a high-bandwidth, internet connected network. Unlike ATAK, which is regularly used on low-bandwidth mesh networks, the Dowding Server typically runs as a cloud-based server hosted in Silicon Valley, CA. As such, most current Dowding users access the server from high speed internet connections within the continental United States. Even Dowding Servers that are not run from the DIU Rogue Squadron headquarters run most effectively when they are able to connect back to the main server regularly for updates.[108] This presents an issue for SOF to use the Dowding Server in a tactical environment, where internet access and high-bandwidth networking are not a given.

---

[107] Imperial War Museums, "What Was The 'Dowding System'?"

[108] Mark Jacobsen, personal communication, August 20, 2019.

Each of these unique projects uses a different approach to bridge the gap between the C-UAS sensor and the useful digital COP. Even though these projects all seek to solve the issue broadly, none of them is designed specifically for SOF units. As such, the unique requirements of a small, dismounted team are not directly addressed.

D. CONCLUSION

Military doctrine requires commanders to understand and apply the concepts of mission command to accomplish their given missions. Key to this success is a clear and accurate understanding of the operating environment. On the contemporary battlefield, asymmetric threats, such as enemy UAS, endanger ground forces in a way not seen in previous years. To protect their units, commanders must develop sensor, collection, and dissemination plans adhering to the Principles of Protection. While current C-UAS technologies have advanced significantly in recent years, no single sensor provides exhaustive detection for all SUAS or all tactical applications.

Additionally, these disparate sensors are rarely digitally incorporated into a single common operating picture that is optimized for the SOF operator. Established technologies, such as ATAK, allow leaders to make accurate, timely decisions and enhance their ability to execute mission command. Advancements in sensor technology allow more accurate and timely detection of SUAS threats. The integration of these sensors and SA tools continues to be the weakest link in the system. While technologies such as the Dowding Server show promise, they have not been tested on realistic SOF missions in austere environments.

By integrating proven UAS sensors into the ATAK system, commanders could enhance their situational awareness and improve the protection of their units. This would be especially pertinent to SOF, as SOF units are inherently smaller, less centralized, and often operate with fewer defensive protective measures. Due to the prolific threat of cheap, effective LSS UAS, it is essential that existing and emerging technologies be integrated and leveraged to fill this capability gap.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EXPERIMENT EXECUTION

To obtain useful data to answer our research questions, experimentation required live testing of situational awareness (SA) tools and counter-UAS (C-UAS) technologies with SOF operators. We accomplished this by conducting our field experiments with the Norwegian Special Operations Command's *Marinejegerkommandoen* (MJK) and the Norwegian Defence Research Establishment (FFI). The MJK is an elite maritime special warfare unit and trusted NATO-SOF partner to USSOF; their interoperability of tactics, techniques, and procedures has been proven for years in training and combat. Because of this partnership history, as well as their capabilities and force structure, we identified the MJK as an archetypal analog for SOF forces writ large.

We leveraged established relationships with the Defense Threat Reduction Agency (DTRA), Defense Innovation Unit's Rogue Squadron (DIU-RS), and the U.S. Army Special Operations Command (USASOC) G8, to design and resource an experimental setup to answer our research question: **How can tactical situational awareness tools enhance decision making and survivability of SOF teams in an enemy SUAS-enabled environment?**

A. DESIGN CONSIDERATIONS

Asymmetric Warfare Group's (AWG) 2018 Defense-in-Depth Exercise (DiDEX) served as the underpinning for best practices when developing our experiment. While DiDEX brought together multiple C-UAS system vendors and conventional Army forces to explore "best practices for employing multiple CUAS capabilities against a low, slow, small UAS threat," our experiment sought to dive deeper into the SOF specific requirements of C-UAS technologies.[109]

To isolate the variables related to our research question, our testing was purposefully designed to place less emphasis on the efficacy of the SUAS sensors themselves and instead focus on the operator's situational awareness requirements as

[109] Asymmetric Warfare Group, *DiDEX 2018 Final Report*, 8.

they applied to SUAS detection. We accomplished this by selecting a single sensor for all iterations of the experiments, conducting all tests within the range of the sensor, and flying SUAS listed in the RF library of the sensor.

The detection and networking technologies used in the experiment were selected based on their availability and widespread use within USSOCOM. This was done to maximize the generalizability of our results to current SOF units. A diagram depicting all hardware and network equipment used during experimentation, with iconography, can be found in the Appendix.

B. EXPERIMENT FRAMEWORK

The experiment was divided into four phases: equipment and network bench tests, Dowding Server implementation, tactical field experimentation, and full mission profile experimentation. Each of the first three phases were divided into iterative and incremental subphases to ensure critical tasks were accomplished before the culminating experiment in Phase 4. Phases 1 and 2 were conducted locally and focused on meeting critical gateways to ensure viable and productive experiments during Phases 3 and 4. The final two phases consisted of two days of field experimentation in Bergen, Norway and sought to answer our research question through the execution of multiple scenarios varying in type and complexity. Table 3 lists the experiment phases and subphases.

Table 3. Experiment Phases

Phase 1—Equipment Downselect and Network Bench Tests
Subphase A: TAK Bench Tests and MANET Connectivity
Subphase B: SUAS Familiarization
Phase 2—Dowding Server Implementation
Subphase A: Dowding Familiarization, Simulation, and MANET Operations
Subphase B: Dowding, ATAK, and SkyView Integration over MANET
Phase 3—MJK Tactical Reconnaissance and Direct Action Testing
Subphase A: Tactical Reconnaissance Mission Using ATAK
Subphase B: Tactical Reconnaissance Mission Using Dowding
Subphase C: Direct Action Mission Using Dowding
Phase 4—MJK Maritime Special Reconnaissance Experiment

C. PHASE 1—EQUIPMENT DOWNSELECT AND NETWORK BENCH TESTS

The purpose of Phase 1 was to establish consistent connectivity for all Android devices over the MANET and to familiarize the team with the operation of SUAS. Critical to this phase was establishing and maintaining a functional MANET, mastering ATAK operations, and certifying the SUAS pilot. At the end of Phase 1, the team was capable of operating situational awareness tools over the tactical MANET, and prepared to begin the integration of C-UAS sensors. Table 4 lists critical objectives by subphase.

Table 4. Phase 1 Objectives

Phase 1—Equipment Downselect and Network Bench Tests
Subphase A: TAK Bench Tests and Mobile Ad Hoc Network Connectivity
Objective 1: Establish communication between ATAK using various WLAN setups
Objective 2: Determine feasibility of MANET configurations for Phases 3 and 4
Objective 3: Train the team on ATAK operations
Subphase B: SUAS Familiarization
Objective 1: Familiarize team with SUAS operations
Objective 2: Train and certify SUAS operator

1. Phase 1A—TAK Bench Tests and Mobile Ad Hoc Network Connectivity

The purpose of Phase 1A was to establish communication between ATAK-enabled Android tablets and Samsung cell phones using a wireless local area network (WLAN), and determine the feasibility of these networks for use in future experimentation. Once the Android devices were connected to the network, a simple communications test was conducted on each device. A successful test was determined if the device was able to accomplish two tasks: send and receive ATAK text messages with the other user and manually populate icons to a shared COP. The devices were bench tested using the following network set-ups (Figure 7).

- Infrastructure mode WLAN
- Closed, persistent mobile ad hoc network (MANET)
- Persistent MANET with internet gateway
- Intermittent MANET

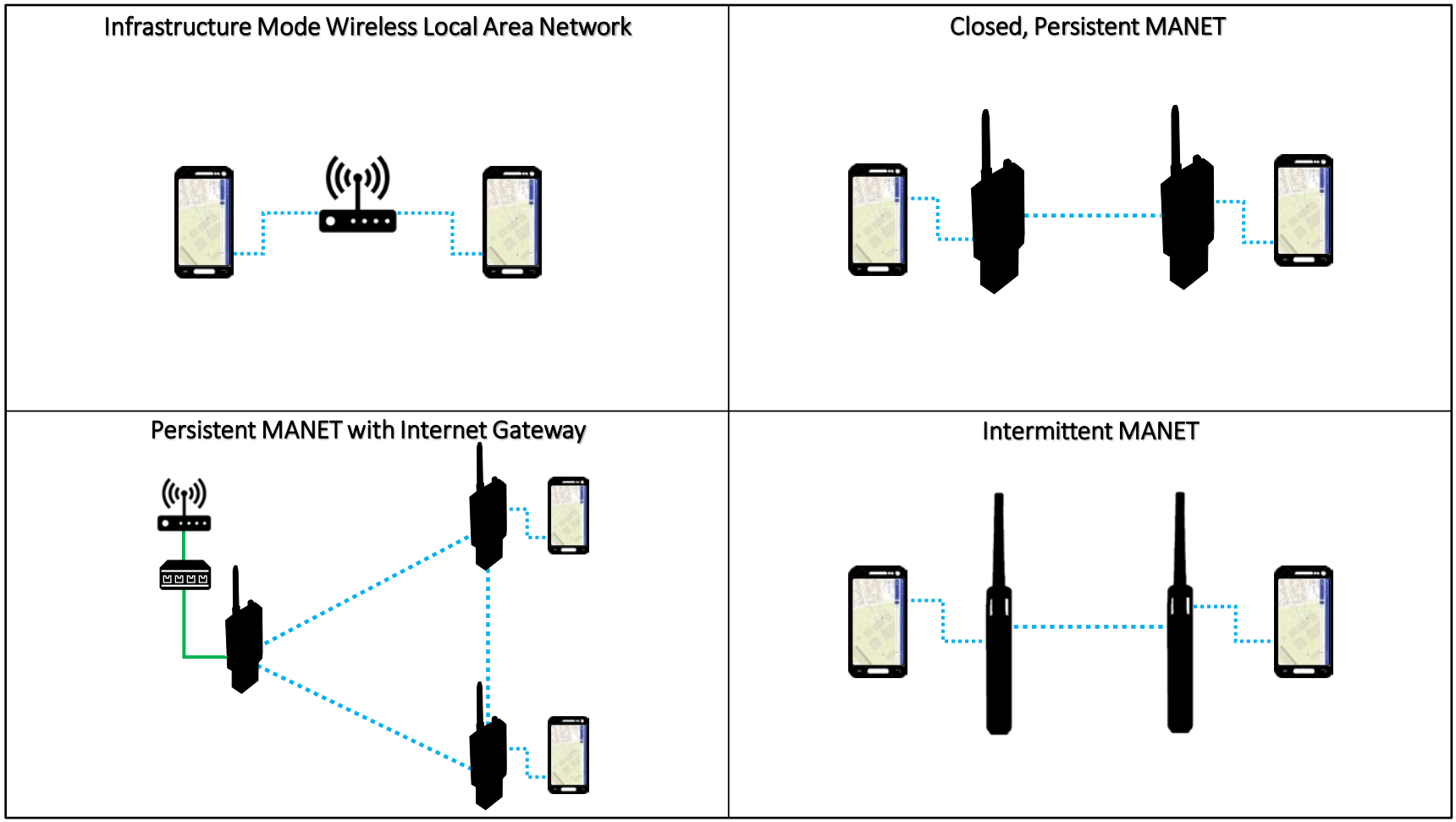


Figure 7. Phase 1 Network Diagram

a. Actions

A mobile Wi-Fi hot spot was used to establish the infrastructure mode WLAN. Both tablets were connected to the same hotspot using the wireless access point (WAP) hub and then tested.

To establish the closed, persistent MANET, two MPU4s were configured to use 2 Watts and operate at 2.462 GHz. The MPU4 and MPU5 radios are "software defined" which allows a trained communicator to program the radio for desired power use and set the time between transmitted and received signals. After initial setup, we made no modifications to MPU4 configurations for the remainder of the experiment. Each Android tablet was then connected to its assigned radio using the MPU4's WAP feature and then tested.

The persistent MANET with internet gateway was established by adding an additional MPU4 radio, a small network switch, and a Long Term Evolution (LTE) router to the closed, persistent MANET. The additional MPU4 was hard-lined into the network switch with the provided network cable adapter; the LTE router was then connected to the network switch using CAT-5e cable. The devices were then tested for ATAK communication capability, and the ability to access the internet.

Following successful testing of the persistent MANET, the MPU4 radios were replaced with modified MPU5 radios and the test was repeated. Each MPU5 radio used throughout the experiment was modified by adding a SNMP plug-in agent programmed to record network performance and provide WAP capability (a feature removed in the transition from MPU4 to MPU5).

GoTenna Pro radios were used to establish an intermittent, or "bursty," MANET. These radios allow the transmission of short (roughly 250 ASCII characters) messages up to 47 miles. While the amount of transmitted data is extremely small, the radios allow the user to establish nearly undetectable MANETs over much greater distances than the MPU series radios.

Following the series of network bench tests, the team conducted detailed familiarization and training with the ATAK. Previous conferences with MJK leadership

determined that many MJK operators had previous experience with ATAK, but their level of familiarity varied greatly; this objective served to mitigate this variable by ensuring members of the team were capable of instructing MJK operators on the proper use of the ATAK during Phases 3 and 4.

This training included updating the firmware on all ATAK devices, managing team and user preferences, and in-depth exploration of the platform's most commonly used capabilities. Each device was set to default configurations and moved applications to the home screen for ease of use. The TAK software relies on internet access to download updates, plug-ins, and maps. In anticipation of operating in an austere environment with only remote access to the internet, offline Norway maps were loaded onto all devices.

b. Observations

During Phase 1A, all objectives were achieved. All tested devices made positive communications tests using all network configurations without issue, with the exception of the persistent MANET using modified MPU5 radios. This error is discussed in detail in subsequent sections.

(1) Persistent MANET

While testing the MPU4 and MPU5 radio networks, the only observable difference occurred when testing the modified MPU5. While using MPU4 and unmodified MPU5 radios, all devices communicated without error; when using the modified MPU5 radios, ATAK messages were not sent out from one MPU5 node to the other. Through subsequent testing, it was determined that, while a networked ATAK device could receive data on the modified MPU5 network, an error in the programming of the SNMP plug-in agent did not allow CoT messages to leave that MPU5 node. While this would limit the full functionality of the ATAK in future testing, it would still allow ATAK devices on modified MPU5 MANET to receive data from SUAS sensors.

(2) Radio Ranges and Software Configuration

While not observed during bench testing, the MPU5 has a greater range than the MPU4 radio, but software configurations and terrain affect the maximum range. Because

the scope of Phase 1A did not encompass network performance at these maximum ranges, the team did not foresee how the initial MPU radio configurations selected would affect the future phases of experimentation. The decisions made in these earlier phases both facilitated and limited our experiments. Though it was assumed that network connectivity would vary over terrain and distances, the abnormalities in network performance due to differences in software configuration were not anticipated. These issues affected overall MANET performance, which ultimately altered experiment results. These limitations will be discussed further in Chapter IV.

(3) MPU Wireless Access

Although pairing Android devices using a WAP to the MPU4 and modified MPU5 radios is a simple process, the connection between the radios and Android devices created an unnecessary point of technological failure that could be solved using a simple, hardwired adapter. Hardwired connections are physically more resilient, especially for the dismounted SOF operator. The WAP also poses a security threat due to the constant frequency emissions between radio and device, while a hardwired configuration removes the radio frequency signature. This issue will be discussed further in Phase 2.

(4) Intermittent MANET

ATAK enabled devices conducted successful communication tests using GoTenna radios without issue. Though this MANET setup worked consistently throughout testing, the minimal volume of data in each transmission was a point of concern, as at this phase of experimentation, the amount of data passed by the SkyView sensor and the Dowding Server had not been determined. Additionally, devices paired to both a persistent and intermittent MANET defaulted to transmitting and receiving over the GoTenna radio, and would not allow the device to access the MPU network. Because of these issues, the intermittent MANET was determined to be unfeasible for future phases of experimentation.

(5) ATAK

The Android devices owned by the Center for Network Innovation and Experimentation (CENETIX) were operating on various outdated versions of the TAK

APKs. TAK allows any person with a software development kit to create a plug-in, making the TAK system flexible and incredibly useful; however, as discussed in Chapter II, not all plug-ins are compatible with the different firmware versions. Baselining all devices to a common firmware controlled the variability between the devices and established a single standard for any required plug-ins.

The realization that the ATAK's maps would be severely limited when operating without internet access provided an important discussion point for other SA technologies. This would later lead to DIU's creation of the "Offline Maps" function for the Dowding App, enabling the use of pre-loaded maps.

2. Phase 1B—SUAS Familiarization

To enable SUAS operations during Phases 3 and 4, the team conducted and observed SUAS training at the Fort Ord Combined Arms Collective Training Facility (CACTF).

a. Actions

The team met with Dr. Kevin Jones, the lead for UAS integration at NPS and a professor in the Department of Mechanical and Aerospace Engineering, at the Fort Ord CACTF. The team conducted familiarization flights using a Ryze Tello SUAS, depicted in Figure 8, to master controls and behavior of the aircraft in an urban training environment.

Figure 8. Ryze Tello Drone with DJI Avionics Next to Controller and Phone

Next, the team moved to a rural training area where Dr. Jones demonstrated high-performance drone flight and discussed best practices and techniques operating SUAS in various environments. Finally, the group discussed UAS research conducted by NPS and how our research focused on the C-UAS aspect of detection and situational awareness.

b. Observations

Although the Tello is much smaller than the Mavic and Matrice models, the flight controls are nearly identical. The Tello and Mavic model SUAS are also both Gyro-stabilized quadcopters that use DJI technology. While they offer different levels of endurance and peak performance, these drones behave similarly to control input. These technologies also allow both aircraft to hover without user control, which drastically impacts the ease of flight. The Tello's controls were intuitive, responsive, and would later prove to be very similar to drones used in subsequent phases.

Throughout this phase, the team gained a greater appreciation for the requirements to fly commercially available SUAS, as well as the function they provide a user. The SUAS used during this phase are similar in capability to those used by enemy forces in conflict zones. By testing these drones in different situations, the team was able to better understand the information SUAS can provide an enemy, and were able to confirm the limitations of the equipment and the requirements of the pilot for conducting these operations.

D. PHASE 2—DOWDING SERVER IMPLEMENTATION

The purpose of Phase 2 was to build and test the experimental setup to be used in Phases 3 and 4. Critical to this phase was development of a fully functional Dowding Server machine capable of operating over a closed MANET and integration of the SkyView C-UAS sensor into the Dowding Server and TAK environment. Table 5 lists critical objectives by subphase.

Table 5. Phase 2 Objectives

Phase 2—Dowding Server Implementation
Subphase A: Dowding Familiarization, Simulation, and MANET Operations
Objective 1: Operate the Dowding Test-Server on a MANET
Objective 2: Simulate SUAS flights over Dowding while on a MANET
Objective 3: Conduct initial testing of NPS-Dowding Server machine
Subphase B: Dowding, ATAK, and SkyView Integration over MANET
Objective 1: Integrate SkyView sensor with the ATAK and Dowding Server
Objective 2: Identify capabilities and limitations of equipment when operating on a MANET

1. Phase 2A—Dowding Familiarization, Simulation, and MANET Operations

During Phase 2A, the team tested the Dowding Test-Server, simulation tool, and app over the tactical MANET and began testing the NPS-Dowding Server machine. The purpose of this experiment was to familiarize the team with the Dowding System and to establish the feasibility of using the Dowding System on a tactical MANET for use in future phases of experimentation.

a. Actions

During Phase 2A, the Dowding App was loaded onto all Android devices (cell phones and tablets) and the Dowding Simulator program was loaded onto all computers by accessing the DIU-Rogue Squadron C-UAS Products page. Two cell phones, two tablets, and a laptop were networked using an infrastructure WLAN (control) and a tactical MANET (proof of concept). Once networked, the laptop was logged into the Dowding Test-Server and the Android devices were connected to the server using the Dowding App. The Dowding Test-Server was also observed from a desktop computer, connected to the NPS high-speed internet; this served as a control for observing the Dowding App's performance on the tactical MANET. Once all devices were connected to the server, the Dowding Simulator was used to create a simulated drone detection by running the "Dowding-Sim" script from the command line of the laptop. Figure 9 shows a successful simulation on an Android device using the Dowding Simulator. This test was conducted several times to observe issues with connectivity, latency, and to identify discrepancies between the interfaces on the tested devices and networks.

Following the proof of concept, DIU created the NPS-Dowding Server, a laptop loaded with a developmental version of the Dowding Server, that had been optimized for portability and to receive changes from the centralized Dowding Web-Server. The NPS-Dowding Server was designed to test the functionality of the system in more austere environments and would serve as the primary mechanism for Phases 3 and 4 of testing. As seen in Figure 10, the NPS-Dowding Server was bench tested using the same protocols as previous iterations and its performance was examined using a tactical MANET with internet gateway as well as a closed tactical MANET.

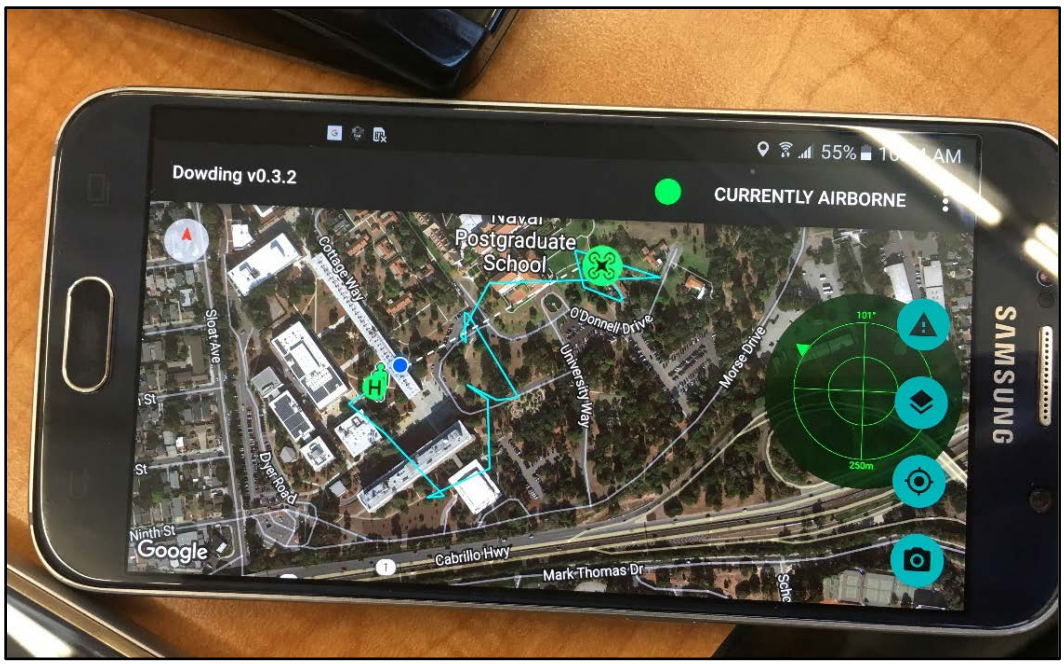


Figure 9. Successful Dowding Simulator Test at NPS

Figure 10. Testing the Dowding Web Server over the MANET at DIU-RS in Silicon Valley

b. Observations

During the Dowding System familiarization and simulation testing, the team made the following observations:

(1) Tactical MANET

For the majority of testing, there were minimal issues with the tactical MANET with the notable exception of the MPU4 WAP connection. During numerous tests, devices were unable to connect to the MPU4 WAP. After using the Wave Relay software to view radio diagnostics, the system had reset the internal clock to January 2000. This desynchronization of the GPS time and the internal clock caused the WAP to reject additional connection leases, which prevented the devices from connecting. To solve the issue, the system was set to "do not renew connection leases" and the internal clock was manually set to 2020, causing all leases to expire. The manual over-ride of the internal clock was then released, allowing additional devices to be connected. While this issue was eventually solvable through relatively simple troubleshooting, it could have been avoided altogether by using a wired connection vice a WAP.

(2) Dowding Test-Server

Throughout Phase 2A testing, the Dowding app and simulator functioned well while connected to the Dowding Test-Server. The functioning Dowding Simulator was critical for the experiment, as poor weather conditions in Norway could potentially prevent UAS flight. When running the simulator, users noted the utility of the radar-like interface that allowed the operator to quickly orient to the drone threat both by distance and direction and the augmented reality (AR) feature that could more accurately refine the drone's position. During simulation, the drone's virtual image as seen using the AR function and the distance and direction provided by the radar interface both matched its simulated location on the Dowding App's COP.

The Dowding Test-Server's overall performance operating on the MANET nearly matched performance with the simulator operating on a high-speed internet connection. Simultaneously comparing the displayed COPs on the different devices, there did not

appear to be a difference in latency between the simulation on the tactical MANET vice the highspeed internet. Icons for simulated detections appeared at nearly the same time on all devices, and the COPs updated at roughly the same rate. Figure 11 depicts the team observing for latency issues.

Figure 11. Observing for Latency Issues Between Dowding Web Application and Dowding over MANET

There was a major discrepancy, however, between the two networks when the Dowding Server required new maps. When a detection occurred in an area without previously cached maps, the Dowding Server used a high-speed internet connection to resolve the maps nearly instantaneously. Conversely, devices connected to the tactical MANET required approximately ten additional seconds to load the same maps; even more time was required to refine resolution to a more zoomed in location. This is noteworthy, because these differences in time were observed under ideal conditions. Each node of the

tactical MANET likely had one-hop access to the broadband router and had multiple routes to access the gateway because of the network proximity during this phase of testing. In a more realistic test, a node may be only connected to one other node and that node may not be directly connected to the internet gateway. Although latency was not a major issue during this test, it was determined that the Dowding App would require an offline map function to be useful in the future phases.

(3) NPS-Dowding Server

When connected to the tactical MANET with internet gateway, the NPS-Dowding Server functioned much the same as the Dowding Test-Server. The only marked differences between the two servers during this test was the ability to use offline maps, which was not used on the webserver, and the ability to see only detections ingested by the NPS-Dowding Server.[110]

The Dowding App and Server became much more unstable when operating on the closed tactical MANET. The NPS-Dowding Server remained suitably stable as long as the network maintained an internet gateway. Without internet connectivity, the server would often display startup errors and failed to allow Dowding App-enabled devices to remain consistently logged in. As such, the experimental design was modified for Phases 3 and 4 to always include an internet gateway.

2. Phase 2B—Dowding, ATAK, and SkyView Integration over MANET

The purpose of Phase 2B was to finalize the integration of the SkyView sensor by testing the SkyView-Dowding Integration Application (SDIA) using the NPS-Dowding Server and the ATAK, and to identify the capabilities and limitations of the experimental equipment when operating on a tactical MANET. To accomplish this, we tested the system using various network modalities to determine the performance differences and feasibility of future field experimentation.

---

[110] The Dowding Test-Server is a cloud-based server that is used throughout the United States. At demonstrations and tests conducted by DIU-RS, all of the detection information populates on the Dowding Test-Server and can be seen by all devices logged into the server.

a. Actions

All of the software engineering required was completed at DIU Rogue Squadron by LtCol Mark Jacobsen and his team; the field and bench testing over the MANET was completed in the CENETIX lab at NPS.

The SDIA was engineered to complete two tasks: to visually display the sensor's data on the Dowding interface and to simultaneously populate the appropriate icons in the TAK environment. To accomplish this, DIU established parameters within the SkyView's server to push CoT data directly to the Dowding Server using transmission control protocol (TCP). Once the data reached the Dowding Server, the SDIA would run two near-simultaneous tasks: redirect the CoT data across the entire network using user datagram protocol (UDP) multicast and translate the raw CoT into the appropriate language for the Dowding Server to ingest the information. By multicasting the CoT data across the network, SDIA effectively populated the appropriate drone or GCS icons on all connected ATAK platforms. Translating the CoT into the Dowding Server's language enables users of the Dowding WebUI and Android App to view the appropriate icons, and will allow the server to efficiently push information to other applications, such as ATAK or other SA tools, for future use. Figure 12 depicts the SDIA configuration.

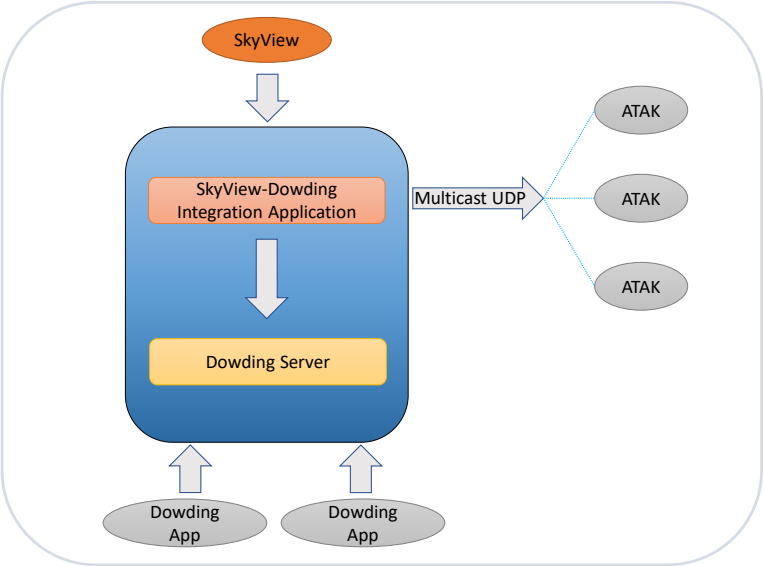


Figure 12. SkyView-Dowding Integration Application

To initiate the SDIA, the user powered on both the SkyView sensor and the NPS-Dowding Server. Once both the sensor and server are powered on, the user inputs the SDIA run command into the terminal of the NPS-Dowding Server machine. The SDIA then connects to the SkyView feed and begins "listening" for outputs from the sensor. All message traffic between the sensor and server are displayed within the terminal window as long as the SDIA is running.

At DIU, the SkyView sensor was networked directly to the NPS-Dowding Server machine using a CAT5e cable, while the NPS-Dowding Server, tablets, and cell phones were connected to the DIU network by wireless access hub. Figure 13 depicts the SkyView configurations and subsequent modifications. The SDIA was bench tested using the SkyView sensor to detect a DJI Mavic Pro Platinum while observers monitored the ATAK and Dowding App using the tablets and cell phones. Following a successful bench test of the SDIA, all experimental equipment was taken back to NPS for operational testing on the tactical MANET.

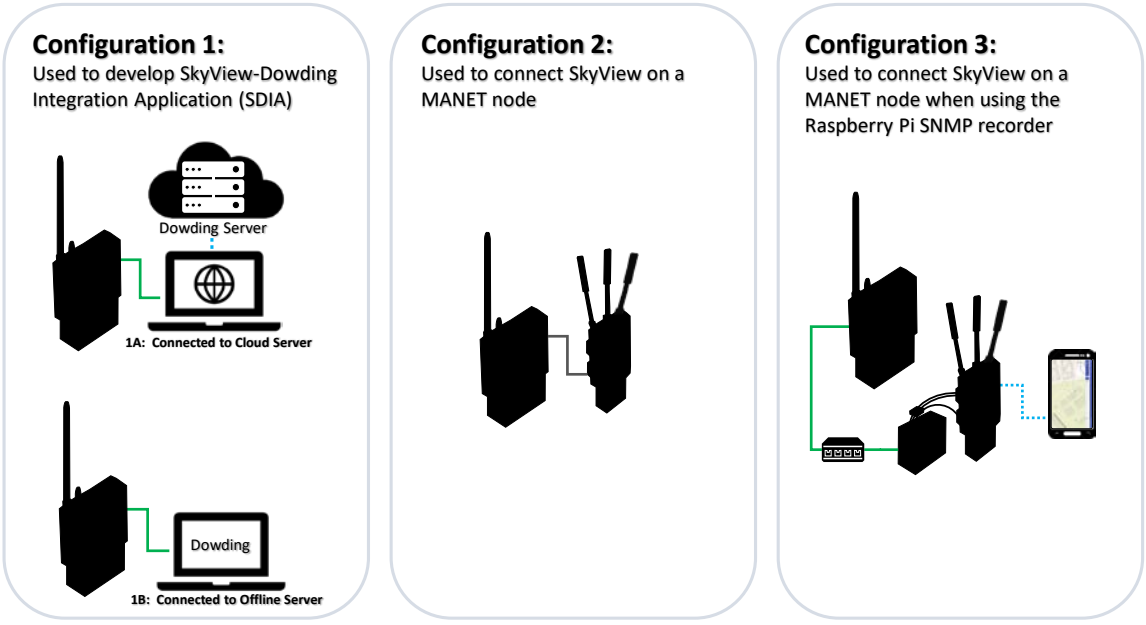


Figure 13. SkyView Sensor Network Configurations

Once back at NPS, the Dowding Server, SkyView sensor, and Android devices were networked into the MANET using MPU4 radios. All tactical MANET nodes remained within 20 meters of each other throughout the experiment. Following a successful connectivity test of the network and all attached devices, the SDIA was tested by using the SkyView to detect Mavic Pro Platinum and DJI Matrice drones while observers monitored the ATAK and the Dowding App from tablets and cell phones. Using the initial test as a base, the system was tested in various network configurations, and other variables were introduced to explore the capabilities of the system and to identify differences in the ATAK and Dowding App interfaces. The following tests were conducted during Phase 2B and are depicted in Figure 14:

- Closed, tactical MANET
- Tactical MANET with internet gateway
- Tactical MANET with internet gateway; SkyView sensor networked as separate node
- SDIA and Dowding Simulator simultaneous operation

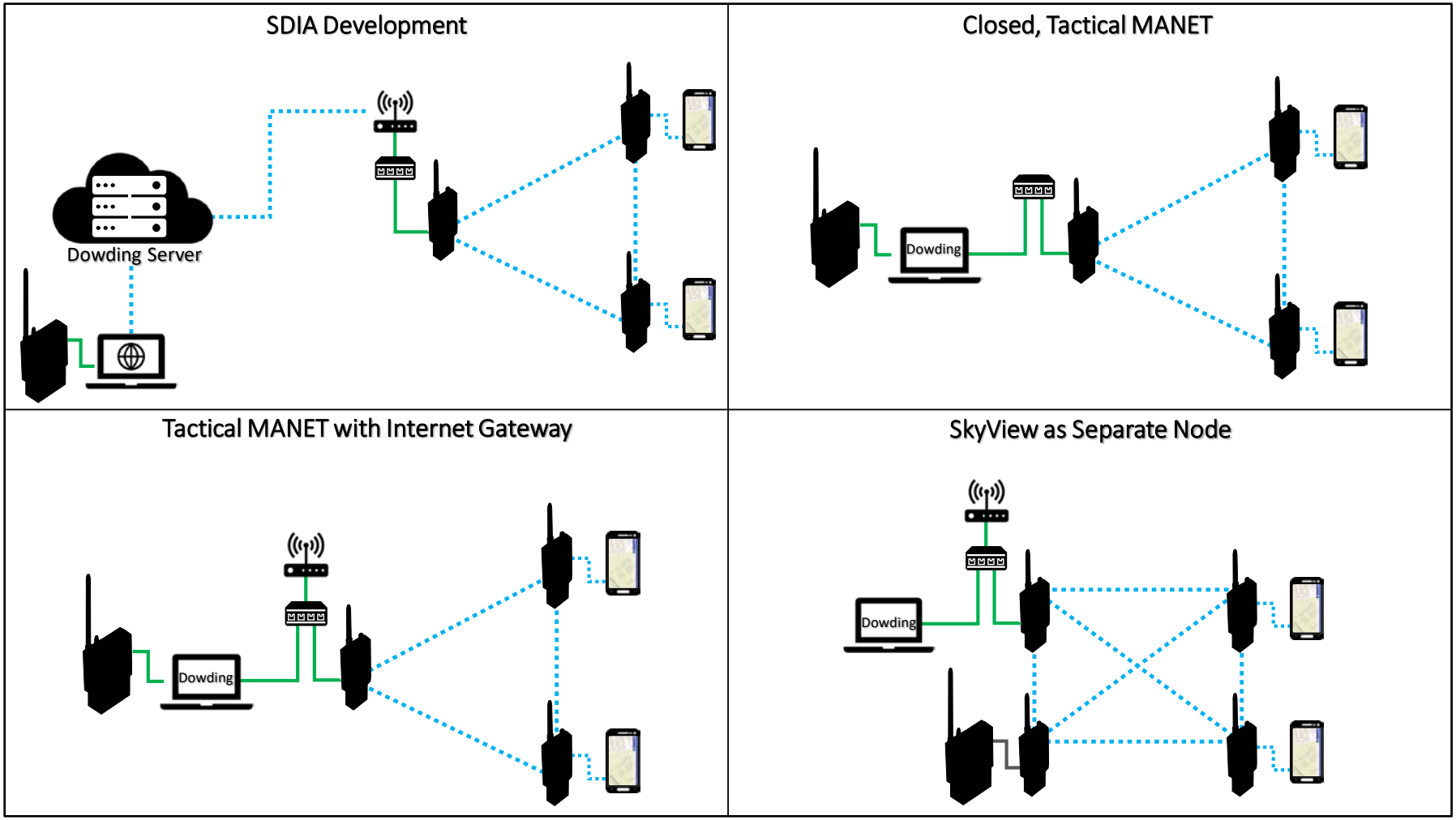


Figure 14. Phase 2 Network Diagram

b. Observations

During Phase 2B, the team made the following observations:

(1) COP Appearance

During the testing on both structured and ad-hoc networks, the SDIA accurately populated icons on both the ATAK and the Dowding App. There was no noticeable difference in the COP appearance between any of the tested network configurations on either application.

When running the SDIA and Dowding Simulator in parallel, the UAS and ground control station (GCS) icons populated from both programs on the Dowding App. Because the Dowding Simulator was not designed to push information to the TAK environment, these icons did not appear on the ATAK.

(2) Alerts

The Dowding App enabled devices to receive timely warnings following a SkyView detection and, at the end-user level, seemed to be unaffected by the network architecture. While using the SDIA and Dowding Simulator concurrently, devices received consistent alerts from both programs without issue.

(3) Latency

Users did not observe a significant difference in latency between the ATAK and Dowding App on any of the tested networks. There was no perceived difference in detection time, latency, or accuracy when the SkyView was networked into a separate node vice directly connected to the Dowding Server. There did not appear to be any delays associated with running the SDIA and Dowding Simulator concurrently.

(4) Indexing the Threat

The Dowding App's augmented reality (AR) and radar interface seemed to function more smoothly when using the Dowding Simulator vice data from the SkyView sensor. Even on a stationary drone, the "drone indicator box" for a SkyView detection was much less stable and more difficult to index. When using SDIA and the Dowding Simulator in

unison, both the AR and radar interface functioned in a manner nearly identical to the independent operation of each program. The presence of an internet gateway made no observable difference in the performance of either the AR function or the radar interface.

(5) Stability

As seen in Phase 2A, the NPS-Dowding Server and Dowding App remained more stable when networked to an internet gateway. Without an internet gateway, the Dowding Server did not function consistently enough for field testing. There was no observable difference in the stability of the Dowding App or the NPS-Dowding Server when both the SDIA and Dowding Simulator were in operation. Neither the ATAK nor the SkyView sensor appeared to be affected by either the network configuration or the presence of an internet gateway.

E. PHASE 3—MJK TACTICAL RECONNAISSANCE AND DIRECT ACTION TESTING

The purpose of this experiment was to examine the graphic user interfaces (GUI) of the ATAK and Dowding Apps as a situational awareness tool while conducting tactical operations in a high-UAS threat environment. Secondarily, we evaluated the capabilities of the SkyView RF sensor as part of an integrated C-UAS system. Table 6 lists critical objectives by subphase. This experiment supported the following research questions:

- How can the integration of C-UAS sensors with tactical situational awareness tools enhance decision making and survivability of SOF teams?
- What factors affect ATAK UI usability in support of C-UAS SA?
- What factors affect the Dowding App UI usability in support of C-UAS SA?

Table 6. Phase 3 Objectives

Phase 3—MJK Tactical Reconnaissance and Direct Action Testing
Subphase A: Tactical Reconnaissance Mission Using ATAK
Objective 1: Examine ATAK SDIA GUI while conducting tactical reconnaissance
Subphase B: Tactical Reconnaissance Mission Using Dowding
Objective 1: Examine Dowding GUI while conducting tactical reconnaissance
Subphase C: Direct Action Missing Using Dowding
Objective 1: Examine Dowding GUI during active, high-intensity operation

1. Participants

The MJK team consisted of one experienced Non-Commissioned Officer from a MJK squadron, while the remaining five operators were recent graduates of the MJK training course conducting advanced training as part of their overall assessment pipeline. Because many of the operators participating in the experiment were new to the MJK, they had little experience with the ATAK system. Unlike the more seasoned MJK operators who regularly use the ATAK and other situational awareness tools, the operators in this experiment had no predisposition to a particular tool. Prior to testing, all operators were issued equipment and familiarized with the capabilities of each item. Each operator was issued an end user device (Samsung S5 or S6 cell phone) with both the ATAK and Dowding applications and an MPU4 or MPU5 mesh radio.

By having SOF operators conduct tactical missions using these different applications, we observed factors affecting a small unit when attempting to gain and maintain situational awareness regarding threat UAS.

2. Site

The testing was conducted at Wolf Camp, a Norwegian Armed Forces training area located in the rural-urban fringe south of Haakonsvern Naval Base. Wolf Camp provided a large, open training space with rolling hills and several buildings. Aircraft during the experiment were cleared up to 400m above ground level (AGL) throughout Wolf Camp.

3. Method

This experiment was conducted in three separate sub-phases. Phase 3A consisted of a simple, tactical reconnaissance mission using ATAK as the primary SA tool. During Phase 3B, the operators conducted the same reconnaissance mission using the Dowding App as the primary tool. During Phase 3C, the team conducted a direct-action assault while using the Dowding App as the primary SA tool.

The Observation Team, consisting of one NPS student and an MJK squadron commander, maintained two large ATAK and Dowding enabled tablets, two MPU5 radios, and the SkyView MP UAS detector. Throughout the experiment, the Observation Team moved with the MJK team and served as the notional higher headquarters for that element. The observation team monitored the actions of the operators, taking note of technical and user interface factors in real time.

The UAS pilots, two NORSOF UAS specialists and an NPS research associate, maintained a fleet of six drones, including a DJI Mavic Pro Platinum, DJI Mavic Enterprise, DJI Phantom 2, Parrot Bebop, Prox Dynamics Black Hornet, and AeroVironment RQ-20 Puma. The UAS pilots were positioned according to their utility and the tactical plan of each iteration.

The Control Team, consisting of two NPS students, maintained the network, ran the Dowding Server, and managed the conduct of the testing from a mobile command center established in an MJK van. The control team's equipment consisted of the NPS Dowding Server (Dell XPS P56F), WinTAK enabled computer (Windows SurfaceBook Pro), MPU4, MPU5, LTE router, and a SNMP agent manager tool. The Control Team remained in the administrative area throughout testing and monitored the COPs using WinTAK and the NPS Dowding Server. Figure 15 shows the Control Team in the mobile command center, and Figure 16 depicts the network diagram for this phase.

Figure 15. Control Team Using Dowding Server (Left) and SNMP Agent Manager Tool (Right) in the Mobile Command Center

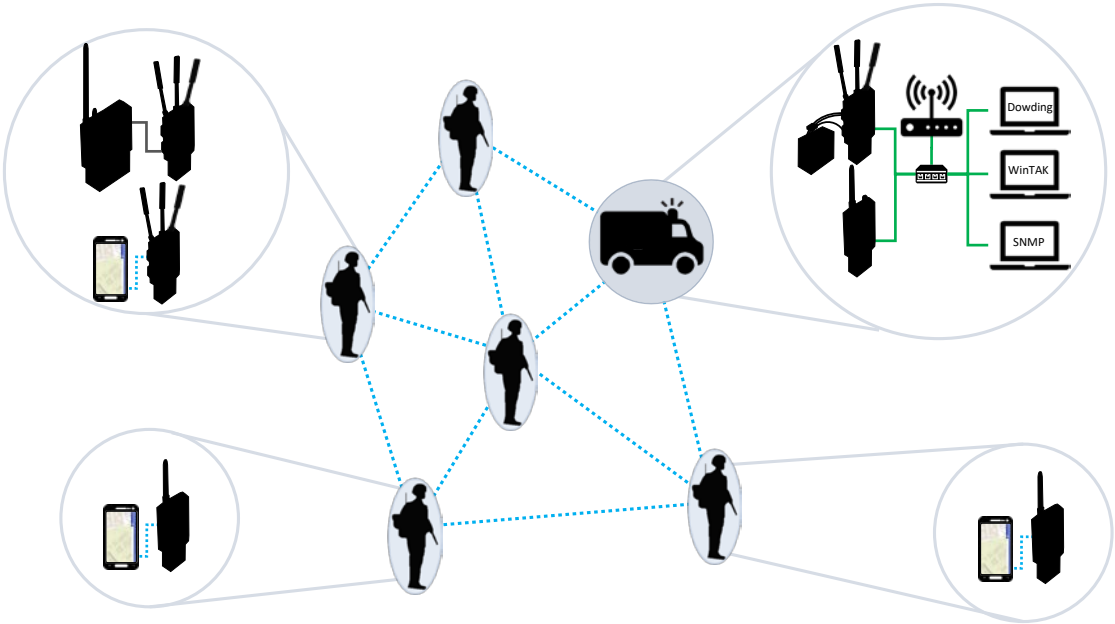


Figure 16. Phase 3 Network Diagram

4. Phase 3A: Tactical Reconnaissance Mission Using ATAK

During this phase, the MJK team leader was given a reconnaissance objective and several minutes to plan an infiltration route and observation points within the training area. Upon completion of planning, the Control and Observation teams tested all issued equipment for functionality and troubleshot any errors with the equipment, ensuring all devices were running both the ATAK and Dowding App, with the ATAK as the active window. Once all equipment was deemed operational, the team conducted a tactical movement to their observation points and began their reconnaissance of the target building.

a. Actions

Once in position, the SUAS pilots launched a DJI Mavic Pro (identified to the team by its location as friendly) and a DJI Mavic Enterprise (not identified to the team as friendly). The friendly SUAS flew as a defensive sensor; the pilot remained 200m behind the MJK element, while the drone itself flew small patterns 100-150m behind the MJK element. As shown in Figure 17, the unidentified SUAS acted as an offensive sensor for the notional enemy forces; the pilot was positioned near the target building, while the drone itself flew aggressive observation patterns throughout the operating area.

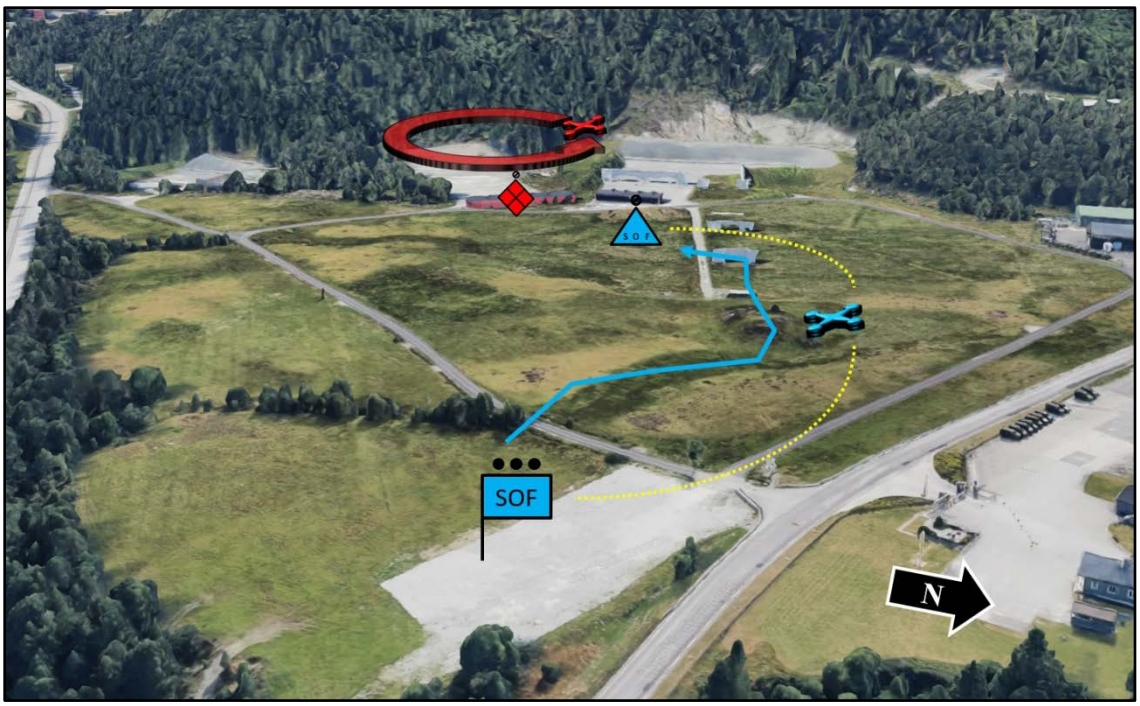


Figure 17. Phase 3A and 3B Concept Sketch

b. Observations

The team made the following observations in Phase 3A.

(1) COP Appearance

While using the ATAK as the primary situational awareness tool, four of the six operators observed both drones and one pilot/ground control station (GCS) icon populated on their individual COP. Two of the operators' COPs only populated one of the drones with its corresponding GCS. As seen in Figure 18, all icons populated as yellow (unknown affiliation) units or equipment and were differentiated by doctrinal unit/equipment modifiers within the icon, as well as a captioned label below the icon. When the operators attempted to manually change the affiliation of the drone or GCS from 'unknown' to 'enemy' or to 'friendly,' the icon would only change momentarily, before returning to its original orientation as the CoT data passed from SkyView would overwrite all of the made changes. Additionally, the ATAK COP only showed the "current" location of the drone, rather than a track of its movement, and did not provide the ability to view previous

detections. This feature will be discussed later, as the Dowding App provides this information.

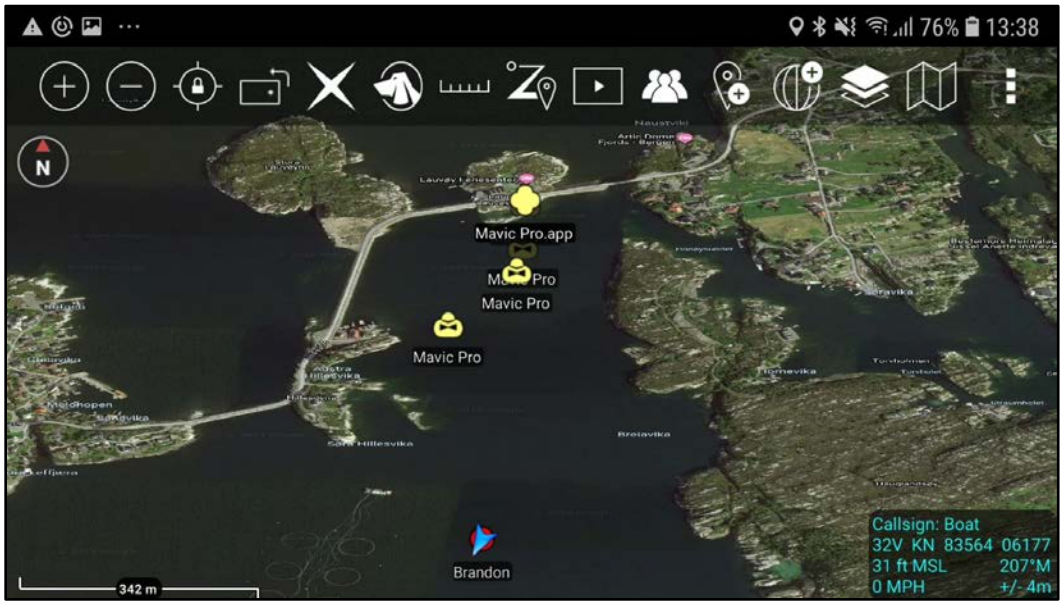


Figure 18. ATAK with Two "Live" Drones, One GCS, and One "Stale" Drone Icon

(2) Alerts

MJK operators noted a lack of alerts within the ATAK interface. While the initial appearance of SUAS icons generally occurred within seconds of the SkyView detection, the system lacked a distinct audible, visual, or haptic warning other than the unremarkable appearance of a SUAS icon. As such, using the ATAK alone required an individual to constantly reference his device to determine the presence of a SUAS. Of note, we observed some operators receive "Push" alerts from the Dowding App while they were using the ATAK as their primary COP; this function is addressed during Phase 3B and 3C. While it is possible to set up a form of alerts by using the ATAK's geofencing function, the operators did not employ this method during the experiment.

(3) Latency

There was a noticeable lag in the movement of the icons as compared to the actual flight of the drone. While we observed SkyView broadcasting CoT data every second (and sometimes more frequently), the operators saw 30-60 second delays in the movement of the icons on their COP.[111]

(4) Indexing the Threat

The delay in icon population, combined with the previously discussed lack of "tracks," made observing subtle drone movements or flight path analysis nearly impossible. Additionally, because the ATAK merely populated an icon on the COP, locating a detected drone in space was not a quick, streamlined process. To visually identify the drone, the operators needed to quickly reference the location of the threat icon against either a feature on the map, such as buildings or hilltops, or by using their location and calculating a general azimuth derived from the COP.

(5) Stability

The operators remarked on the stability of the application. Throughout Phase 3A, the ATAK app continued to run, without a single crash. When the ATAK app lost connection to the network, and thus access to SkyView and other devices, the COP still provided operators some level of functionality, including viewing cached maps, manipulating previously populated icons, and manually placing additional icons.

(6) Overall Assessment

While the C-UAS specific capabilities of the ATAK were limited, the consistency of the application and its usefulness across a variety of missions make it optimal for use in tactical situations. The general situational awareness provided by the ATAK, such as

[111] Delays on the Galaxy phones were much more significant than that observed on the Observer Team's own tablets. While the Observers' tablets maintained a consistent delay under 30 seconds, some of the operator devices only updated once a minute or slower. This may be attributable to the MPU4 radios, which stopped functioning entirely after this iteration.

locations of teammates, the ability to communicate within the app, and ability to manually place icons on the COP, allowed operators to use the app in various scenarios.

5. Phase 3B: Tactical Reconnaissance Mission Using Dowding

This subphase was nearly identical in construct to Phase 3A, with the exception of team size, and the use of the Dowding App as the primary situational awareness tool. Due to significant technical issues with the MPU4 radios, the size of the maneuver element was reduced to the team leader and two additional operators.[112] Actions during Phase 3B mirrored the actions in the previous phase. Both friendly and enemy UAS flew patterns similar to those seen in the previous phase; Observation and Control teams maintained their previous positions. Since both Phase 3B and Phase 3C used the Dowding App, observations have been consolidated in the more complex Phase 3C.

6. Phase 3C: Direct Action Mission Using Dowding

Unlike the first two subphases, Phase 3C focused on the use of situational awareness tools during a more active, high-intensity operation. During this subphase, only three of the six operators received radios and SA devices (the team leader and his two assistant team leaders). The team leader was given a mission to raid an identified enemy building and provided several minutes to plan the conduct of the operation. After briefing his team, the Control and Observation teams tested all equipment for functionality and troubleshot any errors, ensuring the Dowding App was running and viewable as the main window. Following the checks, the team conducted a tactical movement to the target building, established an outer cordon, and cleared the building. Once clear, the team established a hasty defense and was ordered to return to their starting point as depicted in Figure 19.

[112] During Phase 3B, we observed significant issues maintaining a connection to the Dowding Server using MPU4 radios. After troubleshooting for an extended period of time, we decided to reduce the number of operators and use only MPU5 radios, which were not experiencing the same issues.

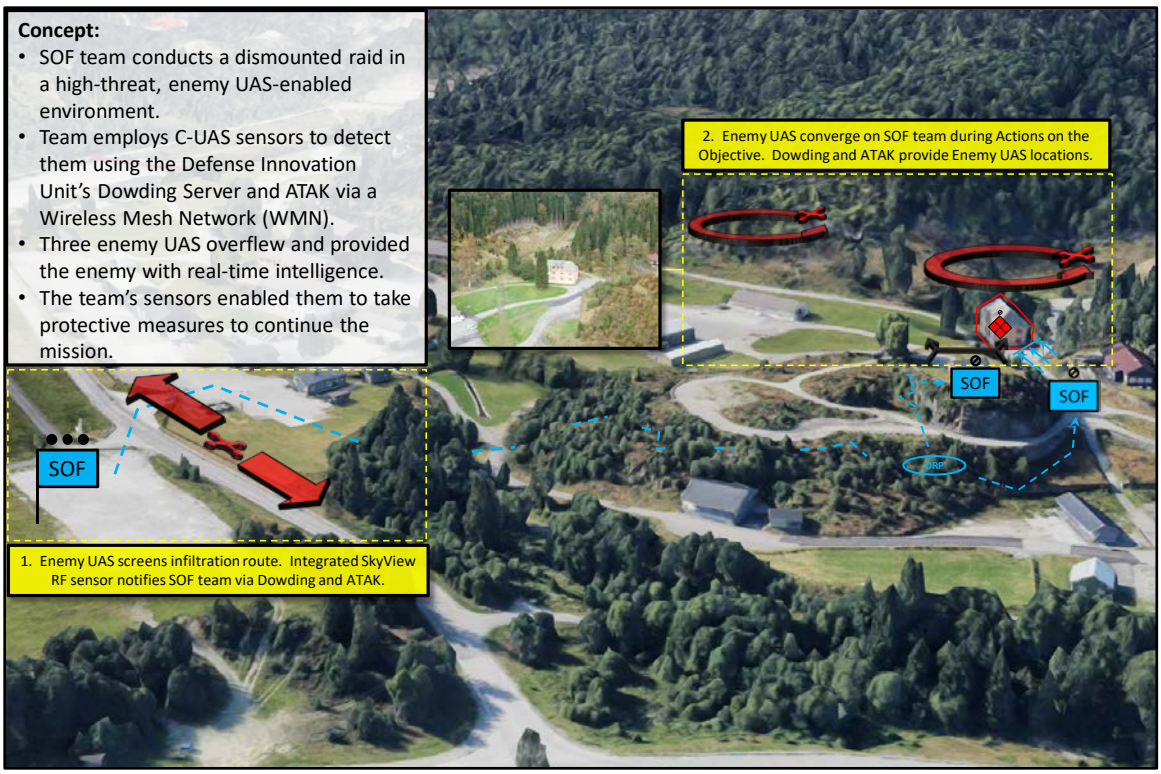


Figure 19. Phase 3C Concept Sketch

a. Actions

During this iteration, the UAS pilots began flying as soon as the team began their movement and continued to fly throughout. The team was briefed that there would be no friendly UAS during this operation. UAS pilots flew sorties of three different aircraft. The DJI Mavic Pro acted as an offensive sensor for the notional enemy forces; the pilot remained in the administrative area, while the drone followed the team's movement and then circled the building once the team was inside. The DJI Mavic Enterprise acted as a defensive sensor for the notional enemy forces; the pilot was positioned 100m behind the target building, and the drone flew sweeping patterns around the far side of the target building. The Parrot Bebop was launched once the team had reached the target building and acted as an offensive sensor for the enemy forces. The Control Team also launched two simulated drone contacts that originated near the target building and flew random patterns in the target area.

b. Observations

The operators were directed to use the Dowding App as the primary SA tool for all iterations of Phases 3B and 3C of the experiment. Compared to the ATAK, the Dowding App provided several C-UAS-specific capabilities that were useful in enhancing SA during both iterations.

(1) COP Appearance

The Dowding App COP presented a simple, clean appearance. All functioning Dowding devices populated icons for both drones and their corresponding GCS. Unlike the doctrinal icons displayed in the ATAK, in the Dowding, drones were represented by colored, circular icons with small quad-copters in the center, while the GCS was represented by a person of the corresponding color. Figure 20 graphically depicts the Dowding App's user interface. This marked difference in appearance allowed the operators to differentiate between the GCS and the drone, with a quick glance at their device.

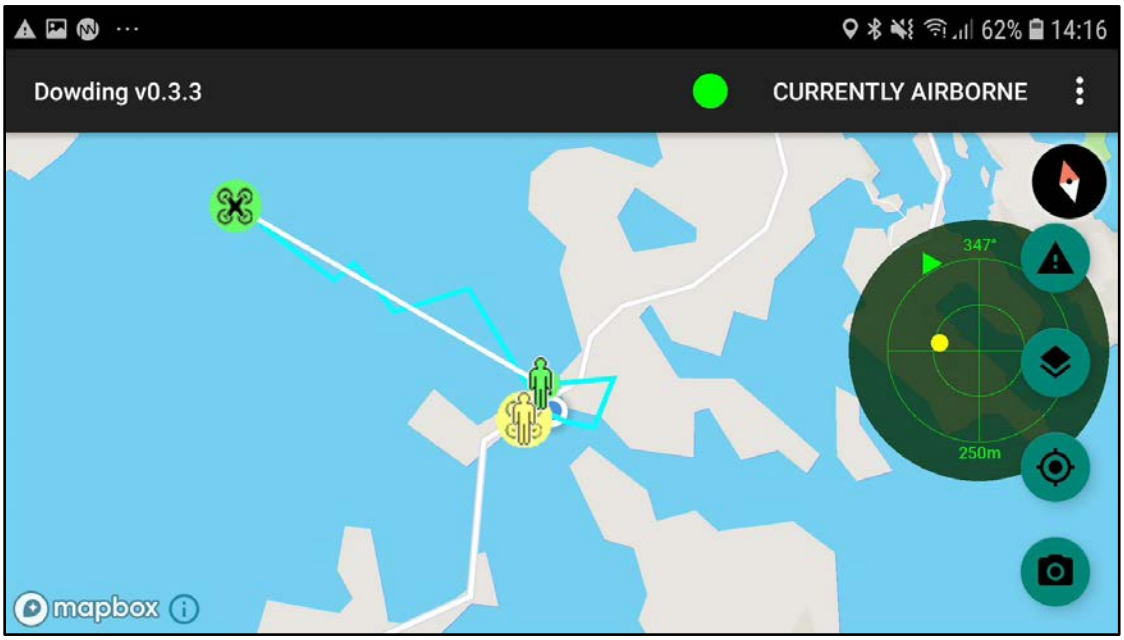


Figure 20. Dowding App with Both Unknown (Yellow) and Friendly (Green) Icons

Additionally, Dowding provided real-time tracks of the detected drones, enabling the operators to see the pattern already flown. The app also allowed users to view historical detections for a specific time block, which was useful for both hasty analysis while on target and for debriefs after the mission. Though the ability to see a drone's previous flight path was very useful both during and after the operation, the tracks of a single drone flight would often appear as multiple, segmented flights, rather than a continuous single track.[113] This inconsistency appeared to confuse the operators and resulted in the team leader misreporting the number of drones in the area.

(2) Alerts

The Dowding App alerted the operators to the SkyView detection of a nearby drone, by providing an audible alert, a visual "pop-up" box, and device vibration to gain the attention of the user. This function alerted the operators to a SUAS threat without requiring them to look at their SA device.

(3) Latency

Both the operators and observers experienced a significantly more up-to-date COP when using the Dowding App vice the ATAK. During Phase 3A, we observed 30-60+ second delays between COP updates; with Dowding, we rarely observed more than 15 seconds of latency and generally observed updates in near real-time. This consistent information flow allowed the team to more accurately identify and report the locations of drones throughout Phases 3B and 3C than they did in Phase 3A.

(4) Indexing the Threat

The Dowding App maintains a self-orienting, radar-like display that allows operators to quickly identify the location of the threat in the air without manually manipulating the map. This feature appeared to be extremely useful while conducting

[113] It is unclear whether this was a function of Dowding interpreting the SkyView data as a new flight, or SkyView losing its "lock" on a drone and then re-detecting the same aircraft and reporting it as a "new detection."

decisive action operations, like Phase 3C, when operators needed to identify and locate a threat in a minimal amount of time.

When using Dowding's Augmented Reality (AR) function, the operators were able to locate the "drone indicator" box, but the box rarely accurately correlated to the location of the detected UAS. Often the reported elevation of the drone was significantly different than the actual elevation, resulting in the "drone indicator" box presenting the drone as on the ground when it was, in fact, more than 100 feet in the air. Though the operators expressed potential utility of this function, in practice, the capability was more distracting than useful in identifying an airborne threat.

(5) Stability

The most notable issue observed during the experiment was the general instability of the Dowding App. While the server itself remained up and active through the entire exercise, a majority of our Dowding App devices lost connection to the server intermittently throughout the day. The Control and Observer Teams experienced this issue regularly during three actions: toggling between historical tracks and live detection, switching from the ATAK to the Dowding App after not actively viewing the app for extended periods, and when the operators reached the edge of their radio's range.

Additionally, we observed several instances when the app crashed upon initial UAS detection as operators manipulated the map to locate the detected drone.[114] Once the app crashed, operators had to restart the app and re-logon to the Dowding Server, a process that the operators were rarely able to quickly complete in the middle of an operation. Upon restarting the app, users observed latent icons and tracks for several minutes, even while receiving current detections. This juxtaposition of current and previous detections confused the operator as to the correct number of drones in the area.

[114] This bug was quickly fixed in a subsequent release of the Dowding App, but we were unable to test the functionality during our experiments.

(6) Overall Assessment

Operators commented that Dowding lacked the general COP functionality that the ATAK provides. The Dowding App only allows users to see their own location and the location of the drones detected by the networked sensor. It does not provide the locations of other Dowding users or the locations of the sensors on the network. As seen with the ATAK, the team noted the inability to manually change the affiliation of the aircraft within the Dowding App itself. As such, all detected drones remained marked as "unknown" icons on the COP, whether or not their association had previously been identified. Overall, the operators found the interface and C-UAS specific capabilities of the Dowding App useful but remarked on the shortcoming of its performance in a field environment.

c. SkyView

While not a specific experimentation objective, we observed and noted aspects of the performance of the SkyView sensor.

(1) Limitations of RF detection

Overall, SkyView consistently detected drones quickly and accurately, providing the location of both the aircraft and GCS for two of the six drones used during testing. Because SkyView is a library-based RF detection device, the sensor did not detect the majority of the drones we employed, including the Puma, Bebop, Phantom 2, and Black Hornet. As discussed in Chapter II, this is a known risk when using only an RF sensor. The sensor can only be as precise as the library of signals loaded into the system.

(2) Detections without appropriate alerts

During one iteration of Phase 3, the SkyView detected the DJI Mavic Pro but failed to identify the GPS location of either the drone or the GCS even though both devices were actively connected to GPS. While the SkyView correctly identified the presence of a drone in the area (and provided an audible "alert" using the provided audio output), because there was no GPS data, no icons populated on either the Dowding App or ATAK user interfaces. This issue represents a significant gap in the integration of SkyView with both of the tested SA tools.

F. PHASE 4—MJK MARITIME SPECIAL RECONNAISSANCE EXPERIMENT

Phase 4 of testing focused on the use of the Dowding App during the conduct of a low-visibility, special reconnaissance missions in a maritime and land-based environment. During this phase, MJK operators used both applications during a full-mission profile training mission. Unlike Phase 3, the experiment participants were all seasoned operators, and members of an organic squadron task-organized into surveillance teams. These operators had previous experience with the ATAK and had undergone familiarization and training with the Dowding App during Phase 3 of our testing.

1. Introduction

During this phase, operators participated in a lengthy surveillance exercise where the threat of enemy UAS was possible. The testing was conducted on the southern portion of Askøy, an island municipality, north of Haakonsvern Naval base, as seen in Figure 21. The operational area spanned roughly 25 square miles of hilly terrain and the inland bays of a North Sea fjord and is scattered with urban villages throughout.

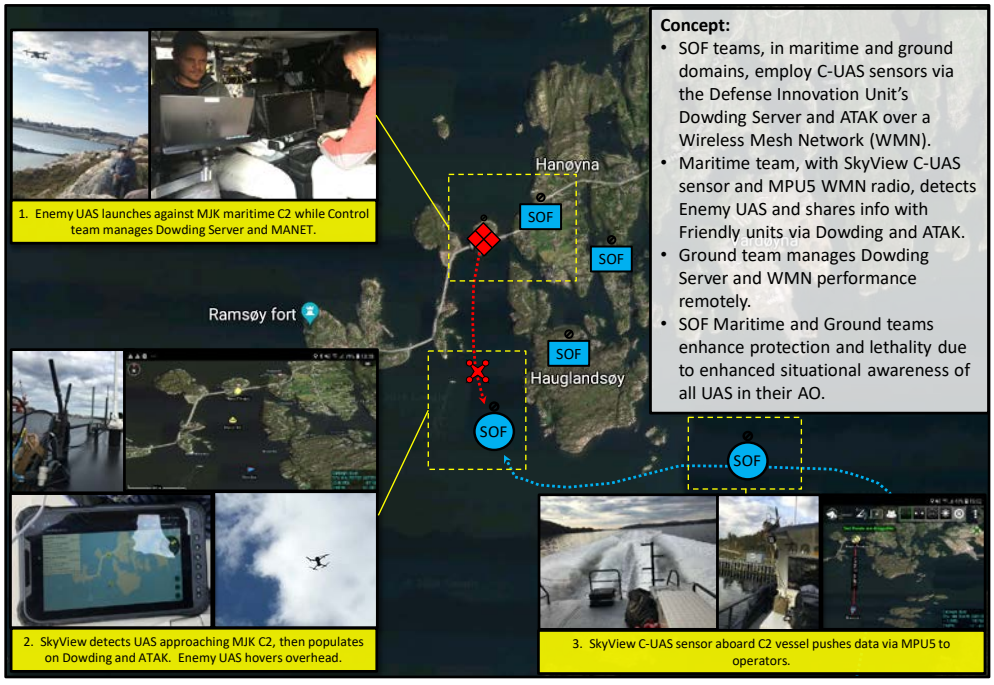


Figure 21. Phase 4 Concept Sketch

The purpose of this experiment was to examine the utility of the Dowding App as a situational awareness tool while conducting low-visibility operations in an environment where enemy UAS presented a threat. Table 7 lists critical objectives. This experiment supported the following research questions:

- How can situational awareness tools enhance decision making and survivability of SOF teams in an enemy SUAS-enabled environment?
- What factors affect the Dowding App UI usability in support of C-UAS SA?

Table 7. Phase 4 Objectives

Phase 4—MJK Maritime Special Reconnaissance Experiment
Objective 1: Examine utility of Dowding as a SA tool during low-visibility operations where enemy UAS present a threat
Objective 2: Examine Dowding performance on a MANET in ground and maritime environments
Objective 3: Examine integration of SkyView sensor on a MANET in a fluid operating environment

2. Method

Because the training event itself was conducted as a single continuous operation, this phase of experimentation was also conducted as such.

The MJK team consisted of 20 operators from an MJK squadron divided into four surveillance teams and a command and control element. Each surveillance team comprised 2-4 operators with low-visibility communications equipment. The teams had mobility platforms in the form of civilian cars or small boats. Before testing, the operators were familiarized with the equipment and operating systems they would use during the experiment. Three of the surveillance teams were issued one MPU5 radio and one end user device for viewing the ATAK and the Dowding Application.

The MJK C2 element consisted of a troop commander and UAS section on a modified 35-foot civilian boat. In addition to their organic communications equipment, the MJK C2 element maintained an AeroVironment RQ-20 Puma UAS, two MPU5 Radios, two large Dowding and ATAK capable tablets, and the SkyView RF detector. Figure 22 depicts the MJK maritime C2 node and network configuration.

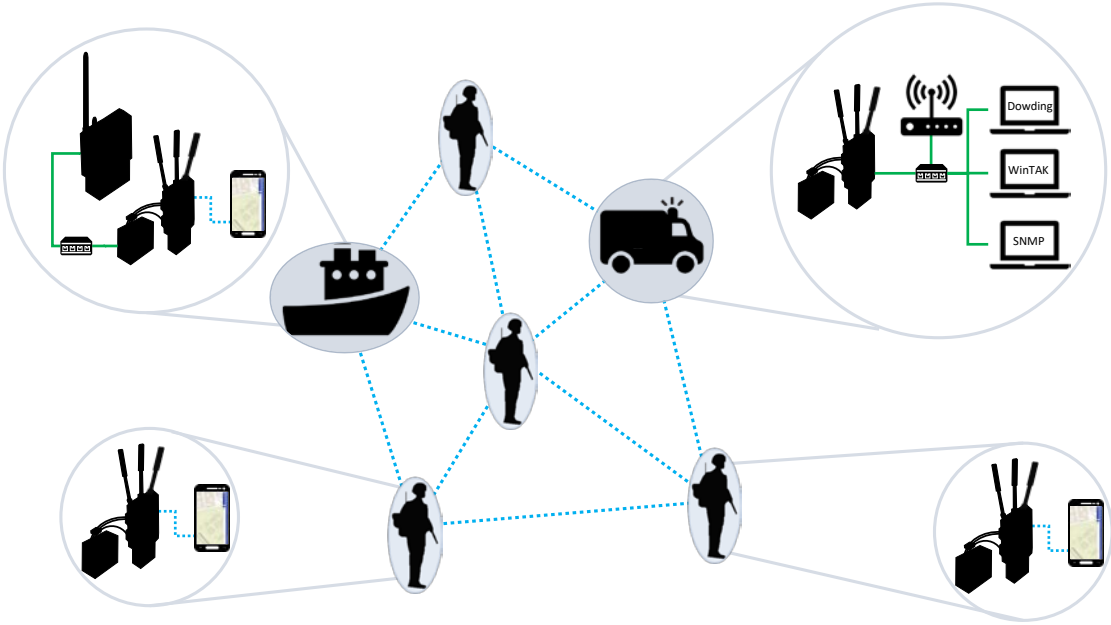


Figure 22. Phase 4 Network Diagram

The Observation Team, consisting of one NPS Student and the squadron commander, were divided between the MJK C2 element and the surveillance teams. The Observation Team used commercial communications infrastructure to relay issues and observations to the Control Team.

The Threat UAS pilots, two NORSOF UAS specialists and an NPS research associate, maintained a DJI Mavic Pro Platinum and a DJI Mavic Enterprise. The Threat UAS pilots were positioned according to their utility within the scenario.

The Control Team, consisting of two NPS students, maintained a network structure similar to the framework used during Phase 3, without the MPU4 radios. The Control Team were repositioned throughout the operation to maintain the mesh network.

3. Scenario

During this phase, the MJK squadron was given a reconnaissance objective, another MJK operator dressed in civilian clothes, and told to maintain visual contact of the individual and to report his route and stops. The targeted individual was to conduct a circuitous, multi-modal movement through the operational area, to include the littoral areas using civilian vessels, and attempt to identify the MJK surveillance.

To accomplish their given mission, the surveillance teams were required to conduct complex, coordinated movements through varied terrain using multiple modes of transportation. The complexity of the operation emphasized constant communication, both within and between the teams, to continuously react to the targeted individual's actions. In the scenario, the operators were not under threat of direct enemy contact, but the mission's success hinged on their ability to maintain visual contact without being identified by the target, raising suspicion from bystanders, or piquing the interest of the scenario's law enforcement or intelligence services.

4. Actions

As the surveillance teams moved throughout the operational area, the Control Team moved to keep the nodes within the mesh network. For the first half of the experiment, rather than trying to pinpoint the surveillance team, launch a threat drone, and have the MJK C2 element detect the drone, the Control Team opted to use the Dowding Server's simulator function to convey the threat of SUAS to the operators. These simulated detections looked nearly identical to the operator when using the Dowding App.

During the second half of the experiment, the Threat UAS pilots launched both Mavic Pro Platinum and Mavic Enterprise drones to detect potential surveillance teams along the main roadway and to identify the MJK C2 element's vessel.

5. Observations

Throughout Phase 4, network connectivity limited the surveillance teams' ability to use the Dowding App. Because of the small number of network nodes and the vast size and dense terrain of the training area, surveillance teams regularly fell out of connectivity with the network. As such, the operators spent much of the exercise without connectivity to the Dowding Server. The network nodes located with the MJK C2 element were the only nodes that consistently connected to the MANET, and thus, the Dowding Server.

(1) COP Appearance

The COP functioned and presented consistently with the observations of Phase 3. The operators noted the simple, easy to read appearance of the Dowding App's interface and remarked on the simplicity of the drone and GCS iconology, as well as the utility of the tracks.

(2) Alerts

During this phase, the Dowding App's alert function was crucial, as operators were balancing their surveillance and mobility tasks with the use of their SA tool. Operators remarked on the speed at which the alerts were presented, as well as the multi-pronged approach (physical, audio, and visual alerts), which indicated the need to quickly reference their SA tool to locate the threat UAS. These alerts were especially useful, given the connectivity difficulties of the over-stretched mesh network. The operators noted that they did not regularly look at the Dowding App, because their devices were not consistently connected to the server. The alert function provided not only an alert that a drone was present, but that their device was back to full functionality.

(3) Latency

The MJK C2 element noted near real-time COP updates, similar to those seen in previous phases of experimentation. Though connectivity issues limited the opportunities for the surveillance teams to observe delays in the COP, they remarked that the icons accurately displayed the locations of the drones and that the COP regularly updated with the movement of the aircraft.

(4) Indexing the Threat

Operators in Phase 4 were less concerned with enemy UAS as a direct threat to the safety of their unit, but rather as an indicator of enemy counter-surveillance. As such, they rarely needed to quickly identify a drone's position in the air, but rather required the drone's location relative to their location or the location of a landmark on the ground. During a surveillance leg, one operator was able to quickly identify a drone in the air by using Dowding's radar-interface. The operators noted the potential utility of the Dowding App's radar interface and augmented reality function, but did not regularly use these features, due to the nature of the mission and the lack of consistent connectivity.

(5) Overall Assessment

During this phase, operators noted the limitations of the Dowding App as a broad use situational awareness tool. Unlike Phase 3, where the primary intra-team communication methods were tactical radio, voice, and hand and arm signals, operators during Phase 4 required the use of low-visibility communications technologies like messaging applications, file sharing, and voice chat-rooms. To ensure each of these technologies functioned properly, the operators used a separate device for the Dowding App and their organic systems. As such, the operators were often fumbling with multiple devices to maintain situational awareness throughout the operation.

Additionally, the operators remarked on the rigidity of the Dowding App, noting the inability to easily tailor the alert types, notification settings, and appearance of the displayed icons. The operators observed instances where drone icons populated in areas outside of their direct influence and were unable to filter those detections from within the app itself. Overall the operators, in this phase, found the Dowding App's alert function helpful but found its utility as an overall situational awareness tool to be lacking.

6. SkyView.

While not a specific experiment objective, we observed and tested several aspects of the performance of the SkyView sensor. During this phase, the SkyView sensor was located on the MJK C2 vessel and connected to the MANET using an MPU5 radio.

SkyView stopped making consistent detections when traveling ~30 knots. When the boat slowed below that speed, the SkyView again began reliably detecting drones. We tested the detection distance by piloting the boat away from an active drone. At 2.3 KM, the SkyView no longer consistently detected the drone. This distance covered was over open water and was measured as a straight-line using the ATAK's measurement tool. Figure 23 depicts the SkyView range test.

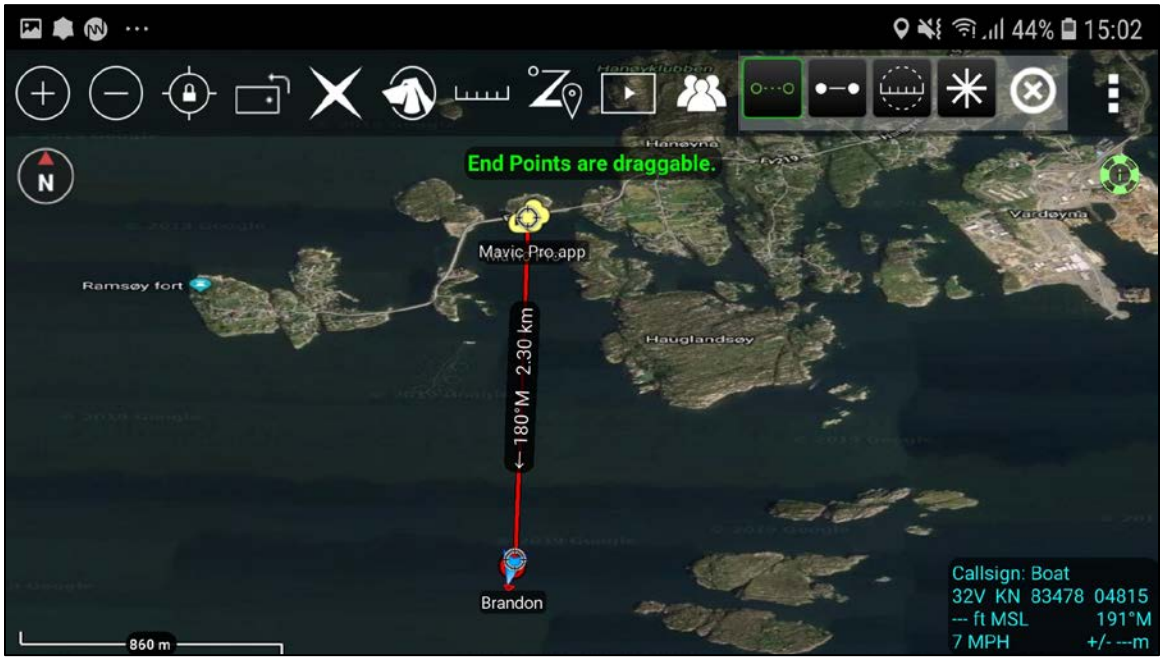


Figure 23. SkyView Detection at 23 KM on ATAK

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

The results of the experimentations fell into two primary categories: capabilities and limitations of the tested tools and utility of the situational awareness tools. While the observations from Phases 1 and 2 are foundational to the overall experiment and useful to furthering comprehension of the state of C-UAS technologies, the data collected from Phases 3 and 4 provides critical answers to research questions. Our research shows that tactical SA tools enhance decision making and survivability of SOF teams by providing operators real-time location data for threat SUAS from networked C-UAS sensors. The following sections illustrate the key C-UAS functions an SA tool must maintain to best support a deployed SOF team.

A. C-UAS SITUATIONAL AWARENESS TOOL REQUIREMENTS

The ATAK and Dowding App, used in conjunction with the SkyView sensor during Phases 3 and 4, provided the operators with real-time SUAS information presented on graphic user interfaces. By observing the team's actions and comments, we were able to determine the factors of each interface that positively and negatively impacted the team's situational awareness and decision making. While the selected SA tools provide operators with similar information regarding the detection of SUAS, we observed several differences that contributed to their ability to make fast, correct decisions without being overwhelmed by the COP or distracted from their tasks.

When conducting an operation under the threat of enemy SUAS, many factors contribute to timely and accurate decision making. During experimentation, we observed four factors critical to a useful SA tool for SOF operators in a tactical environment: a deliberate alert feature, the app's ability to quickly orient the operator to a SUAS threat, flexibility during the conduct of various tasks, and stability of the application itself. While several other factors were identified as significant, these four were consistently recognized as crucial by both observers and the operators themselves.

1. Automated Alerts

This factor refers to the ability to alert the operator to an impending SUAS threat without the operator looking at the device itself. According to many of the operators, this was the most crucial capability for any SA tool, because it enabled them to focus on their required tasks, rather than their SA tool.

Unlike commanding an operation from a Joint or Tactical Operations Center (JOC or TOC), deployed operators must focus on the ongoing task, not on a digital COP presented by an SA tool. As such, an automatic warning function is crucial for operators to maintain situational awareness while conducting complex and challenging mission. The Dowding App's audible warning, haptic vibration, and visual alert window allow operators to focus on the task, and refer to the COP only when notified of a SUAS threat.

The criticality of alerts was most apparent during Phase 3C (direct-action raid) and Phase 4 (low-visibility, special reconnaissance). During Phase 3C, the operators were unable to monitor their SA devices at regular intervals due to the fast pace of the operation, the rapidly changing tactical situation, and the threat of direct enemy contact. While conducting their maritime and land-based special reconnaissance mission in Phase 4, operators became engrossed with the more technical requirements of the operation. During this phase, operators were unable to consistently monitor their COP as they synchronized their movements to maintain visual custody of their reconnaissance objective.

The Dowding App's automatic alerts helped the operators in both phases to maintain SA of SUAS throughout the operation by alerting them to the threat and allowing them to reference the COP during tactically feasible periods in the mission. Without these alerts, the operators would not have been aware of the SUAS threats until they reached a tactical pause in the operation. As such, they would have made decisions using incomplete information, and may have made tactically unsound choices concerning force protection and accomplishment of their mission. The tactical scenarios and missions during Phases 3C and 4 were selected in order to assess SA tool utility across a spectrum of operations. Both experiments underscore the importance of maintaining SA without unnecessarily drawing the operator's attention from their operational requirements.

2. Indexing the Threat

The second critical factor is the COP's ability to identify a SUAS threat and enable the operator to rapidly orient on the location of the aircraft itself. This factor incorporates the features of the tool that affect the efficient nature in which operators receive the information.

The Dowding App's interface enables the user to see the location of the drone on the map and provides real-time distance and direction using the self-orienting radar-graphic. It does this without cluttering the COP with unnecessary information or requiring additional user input (such as clicking the threat icon). The ATAK only provides operators with the location of a detected SUAS by presenting the icon on the COP. Operators were able to determine the distance and direction by using the native "distance/direction" function, but this required several user inputs and was unwieldy in the rapidly evolving situation.

While the Dowding App's augmented reality (AR) feature did not function as seamlessly as expected, a more refined version of this feature could assist users in identifying the exact location of detected SUAS, but would likely not be especially useful during most SOF missions. In its current form, the AR function requires the user to remove his SA tool device from its mount, use both hands to stabilize the platform, and focus exclusively on the device to locate the threat UAS. This capability could prove more useful if incorporated into a heads-up display.

3. Application Flexibility

This factor refers to the ability to use a given application as the primary SA tool when conducting various mission sets and the operator's ability to easily tailor the application to his individual needs. While our experiment focused on the C-UAS utility of a SA tool, the broad applicability of the tool is just as important.

Operators remarked on the limited capabilities that the Dowding System brought to the fight. The Dowding App's C-UAS functionality exceeds those of the ATAK, however, the inability to manipulate the COP and communicate between users, limits its utility as a primary SA platform.

Conversely, though the ATAK features a robust menu of applications that makes it a useful platform as a versatile tool, its native C-UAS functionality is not sufficiently refined to serve as the primary C-UAS COP for SOF units. The TAK platform's ability to host numerous plug-ins adds to the flexibility of the ATAK and could enhance its C-UAS capabilities.

Like the missions they conduct, SOF units and individual operators have unique requirements for mission command and SA tools. While useful as a C-UAS tool, the Dowding App is not sufficiently adaptable to meet the broader needs of the modern SOF operator. During testing, operators commented on the need to quickly change several GUI factors, including alert settings (different audio and visual cues), detection rings (geo-fences), icon filters, drone naming conventions, and the size and appearance of icons. Though some of these changes are possible at the server-level or by using the web UI, none are currently features of the Android app. The ability to quickly make these changes within the app would allow the operator to customize the interface to individual preference and rapidly changing environments.

The ATAK retains much of the functionality sought by the operators during testing; the settings and functions within the ATAK application allow the operators to manually set geofences, filter icons, and to change the name and appearance of icons.[115] While the Dowding App functions as an Android-optimized view of the central Dowding Server, the ATAK application is capable of operating without a centralized server. This setup enables operators to easily manipulate the information presented on their device.

4. App Stability

This factor focuses on a tool's ability to consistently function in an austere environment or when network connectivity is intermittent or degraded. Stability is a critical

[115] Though these functions are all possible using the standard ATAK application, most of these functions either were not used or did work properly during the testing. Operators did not establish or change geofences and they did not purposely filter icons. During Phase 3A, the operators were able to manually change the icon appearance of the detected drones, but the drones quickly reverted to their original appearance due to the nature of the SkyView data.

requirement to SOF units, as unreliable equipment poses too great a risk to operators in high-threat environments.

The operators remarked on the instability of the Dowding App and its inability to maintain a consistent connection to the server. The high latency, intermittent network made it difficult to rely on the Dowding App when conducting high-risk, special operations. During this test, the ATAK remained stable and, although it is not as fast or precise as the Dowding System, was nearly always available.

B. CAPABILITIES AND LIMITATIONS OF EQUIPMENT

This section discusses the capabilities and limitations of the equipment used during the experiment.

1. Tactical MANET

During Phase 4, the radios used to establish our tactical MANET limited our ability to comprehensively test the utility of the selected SA tools. With only five working radios, our ability to stretch the MANET and keep all nodes and devices within the network "bubble" was extremely limited. This number of nodes proved insufficient to maintain connectivity due to the expansive size, undulating terrain, and dense vegetation of the operational area.

The capabilities of the radios themselves proved to be adequate for the technical requirements imposed on them. The bandwidth of both the MPU4 and MPU5 radios was sufficient to sustain the simultaneous data traffic from the Dowding Server, the SkyView sensor, and the ATAK apps. This observation further validates the use of these radios as a data conduit for this type of sensor integration.

2. SkyView

As discussed in previous chapters, the SkyView system is a library-based, RF sensor. While we observed consistent detections to distances as far as 2.3 KM using the SkyView, the sensor is only capable of detecting SUAS pre-programmed into its database. While we controlled for this variable by using only threat drones contained in the SkyView

library during Phases 3 and 4 of experimentation, several SUAS went undetected during preliminary tests. This observation further validates the need for SOF units to maintain a multi-sensor, layered C-UAS capability, as threat UAS not contained in an RF sensor's library will go undetected.

The unique capability of the SkyView is its portability. The model of SkyView tested was designed to receive power from automotive 12V auxiliary outlets, Type B 120V prime power, or various portable military batteries. During field testing, the SkyView was powered by a rechargeable, Persistent Systems battery, allowing an operator to carry the sensor in a backpack throughout the operation. This portability, in conjunction with a robust closed tactical MANET and SA tools, enable the SOF unit to maintain a self-contained SUAS detection capability.

In an environment with denied communications, this capability enhances the small unit leader's ability to exercise mission command, by increasing situational awareness without the resources of his higher headquarters. While we tested the capability of our SUAS detection system on a closed MANET in small-scale experiments during Phase 2, the Dowding System did not perform consistently enough without internet access to evaluate this network configuration during our limited field-testing window. Though our experimental setup using the Dowding Server in conjunction with the SkyView sensor serves as a potential model for a man-portable, closed network C-UAS system, we were unable to fully validate this capability.

Operating a man-portable SUAS detection system on a completely closed MANET comes at a cost. Our research found that the only man-portable SUAS sensors currently available are those that rely on RF detection. As previously discussed, relying exclusively on RF sensors places significant risk on the operators by allowing SUAS whose signals are not codified in the sensor's load set to go undetected. This conundrum requires leaders of small, separated teams to balance the detection requirements with the requirement to maintain a diminished electronic signature.

V. CONCLUSION AND RECOMMENDATIONS

Our research and experimentation identified the necessary factors for a situational awareness tool to be effective for SOF operators in an environment where the threat of enemy SUAS is likely. Using these four critical factors as a foundation, we identified several additional steps that, if implemented, will significantly enhance the mission command and protection capabilities of these SOF units. Finally, our experiment highlights the need for additional research and testing to better integrate C-UAS technology with situational awareness tools.

A. THE FUTURE OF C-UAS AND SA TOOLS:

As discussed in the previous chapter, the key factors for a C-UAS SA tool are a purposeful alert, an ability to quickly convey the spatial position of a threat, the tool's utility when used during different missions, and stability of the platform. By leveraging these factors to drive future development, USSOCOM and the Department of Defense can maximize the effectiveness of SA tools and better prepare SOF leaders for current and future battlefields. This can be accomplished by implementing the following initiatives:

1. Dowding ATAK Plugin

To make ATAK more effective in combatting SUAS threats, the system must be optimized to receive and display the appropriate information. A Dowding plug-in for the ATAK solves the identified problems of the Dowding App's instability and single-mission focus by embedding its capabilities within the stable and diverse TAK environment. Simultaneously, the plug-in would bring nuanced C-UAS capabilities to the ATAK application, bolstering ATAK's utility on the current and future battlefields. This plug-in should incorporate the Dowding App's radar-interface, multi-dimensional alerts, and historical data. Creating a Dowding-based ATAK plug-in would provide the operator with the most useful aspects of both applications and maximize the critical factors outlined in Chapter IV.

2. Further Sensor Integration

The current set of SUAS sensors integrated into the Dowding Server is primarily comprised of RF sensors. Future efforts should focus on incorporating radar and acoustic sensors into the system to ensure SOF units can utilize their entire arsenal of detection capabilities.

3. Multi-Sensor Fusion

With the incorporation of additional sensor ingest protocols, any C-UAS plug-in, Dowding-based or otherwise, must include intelligent software capable of aggregating and filtering data to provide the user with the most critical information. This synthesis is necessary to ensure information is clearly displayed to the user and to avoid multiple reports of the same aircraft, as seen in previous research.

4. Optimize for the Individual Operator

Any C-UAS plug-in for the ATAK should be user-tailorable to the individual operator within the application itself. Users should be able to adjust geo-fences, alert settings, and icon appearance from the plug-in interface using an intuitive option menu. This capability broadens the applicability of the plug-in by allowing users to modify their interface based on individual preference or mission requirements.

B. FUTURE RESEARCH

While the results from our experimentation provided insight into the requirements of SA tools for SOF operators in a C-UAS environment, there is still much work to be done to counter the threat of LSS UAS. Several factors limited our research, including the developmental nature of the tested tools, the limitations of our equipment, and the scope of our research topic. Future research and testing should focus on the following research areas:

1. More Rigorous Testing

To further investigate the potential utility of an integrated C-UAS/SA tool system, the app/plug-in should be tested by various SOF organizations in more demanding and

diverse situations. This testing should include multi-day exercises in austere environments and incorporate airborne, heliborne, and amphibious operations to more accurately simulate SOF missions.

2. Closed Tactical MANET

Additional testing should be conducted relying on a robust, tactical MANET without an internet gateway. Our testing included several bench tests to test this capability, but future field testing should seek to investigate the feasibility of a completely closed tactical MANET as the primary network architecture for a SOF team's C-UAS capabilities.

3. Expand the MANET

In addition to testing a closed tactical MANET, future testing should incorporate long-range, bursty radios into the MANET. Using long-range capabilities, like the GoTenna Pro, could enable dismounted SOF units to incorporate non-portable sensors, such as radars, into their SUAS detection plan. This would allow operators to rely on more than just RF detection, when operating as a dismounted force.

4. SUAS Defeat

While our research focused on the C-UAS aspect of SOF missions, the scope of our testing did not include any defeat capabilities required to truly protect SOF units from a SUAS threat. Future testing should seek to integrate both detect and defeat technologies into the TAK environment to develop and evaluate a comprehensive C-UAS platform. Exploring the integration of these capabilities will further enable SOF leaders to protect their units by providing additional capabilities to deal with SUAS.

5. SUAS Swarms

Though our experimental setup was tested against as many as three live drones simultaneously, we did not explore situations including swarms of drones. Considering the emerging threat of autonomous swarm technologies, future research might address such possible scenarios.

6. Unite Disparate Efforts

If our team learned one thing from our initial research for this experiment, it is that the Department of Defense has countless C-UAS efforts moving simultaneously. While some of these efforts are novel approaches to the LSS UAS problem, many are redundant. Much of this duplicative effort is due to an ignorance of the available technologies and a lack of communication between the organizations that develop them. To reduce the unnecessary resourcing of these technologies, future research should seek to combine the efforts of these disparate projects and incorporate interested parties from across DoD and industry. By uniting these efforts into a more cohesive C-UAS campaign plan, future projects can better support SOF forces in the current battlespace and beyond.

C. LIMITATIONS

This section discusses how the design of the experiment influenced the results and potentially limited the value of these observations. Our experiment was conducted by a single SOF unit (Norway's MJK), executing three mission sets through one to six-hour iterations. While the operation in Phase 4 was relatively complex, the missions conducted in Phase 3 were very simple. The operational complexity was further limited by the size and range of our tactical MANET. As such, the tests did not encapsulate the breadth of SOF missions or the diversity of SOF units.

1. MANET

As previously mentioned, the number of radios contributed significantly to our connectivity throughout Phase 4 of the operation. Because of this, operators during this phase only had intermittent communication capabilities and were unable to reliably use the SA tools, which limited our observations. Additional radios would have enabled us to build a more extensive tactical MANET for testing. A more robust network would have enabled the operators to more easily use their SA tools throughout their operation and provide better data for analysis.

2. C-UAS Sensors

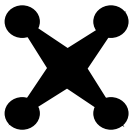
Though we initially sought to incorporate several sensors into the experimental design, we were only able to obtain and evaluate the SkyView. Therefore, we cannot generalize our findings without further testing. Integrating additional sensors into the experiment would have allowed us to examine the utility of a more robustly populated cop, and assess key aspects of data feeds from different sensors. As previously discussed, a comprehensive, multi-sensor battery of C-UAS capabilities is required to best protect military forces from threat UAS.

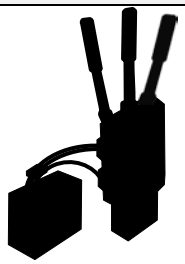
3. Time

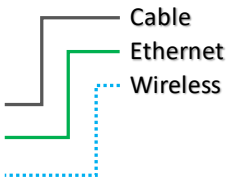
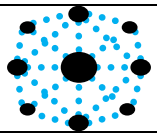
The final two phases of the experiment consisted of roughly three days of testing and observation. While we designed the experiment to incorporate three different special operations missions (static reconnaissance, direct-action raid, and special reconnaissance) across diverse terrain, the available experiment window limited our ability to examine the SA tool utility in other scenarios. This also prevented more iterative testing of the individual experiments to systematically isolate salient factors affecting SUAS situational awareness.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. EQUIPMENT AND NETWORK INVENTORY

C-UAS and Network Items			
NAME	**PICTURE**	**SYMBOL**	**PURPOSE**
Small Unmanned Aerial System (SUAS)			Commercial off the Shelf (COTS) drone with advanced avionics that provides multipurpose capabilities.
Android Tactical Assault Kit (ATAK)			End User Device (EDU) used by operators to access ATAK and Dowding.
Dowding Server	None		System created by DIU to provide C-UAS situational awareness.
Dowding Server Machine	None		Offline Dowding Server built by DIU for expeditious employment in Norway.
Man Portable Unit GEN4 (MPU4)			MANET radio used to communicate via data and voice.
Man Portable Unit GEN5 (MPU5)			MANET radio used to communicate via data and voice.

C-UAS and Network Items			
NAME	**PICTURE**	**SYMBOL**	**PURPOSE**
MPU5 + SNMP Raspberry Pi			MPU5 modified with Raspberry Pi to record SNMP data.
GoTenna			Commercially available “bursty” communications radio.
SkyView MP			C-UAS sensor that uses radio frequency (RF) detection to identify and locate UAS.
4G Broadband Router			Device that facilitates internet access through a data plan.
Network Switch			Hardware that connects multiple devices to a network.

Other Network Symbols		
NAME	**SYMBOL**	**PURPOSE**
Connections		Colors represent the type of connection. Black is any hardwired connection cable other than CAT5e. Green is CAT5e Ethernet cable. Blue is a wireless connection.
Mobile Ad Hoc Network (MANET)		System of wirelessly linked communication nodes that self-configure.
Laptop		Laptop symbol represents any other computer used by the team. The world symbolizes connection to the world wide web. The world symbol was replaced with a word to identify any other functions (i.e., WinTAK computer).
Operator		Operator refers to either a dismounted or mobile (car, ATV) SOF member.
MJK Vessel		A civilian ship modified for SOF command and control.
MJK Van		A civilian van modified for SOF command and control.
Operations Center		A centralized node of people and equipment that enables command and control.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Almohammad, Asaad, and Anne Speckhard. "ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics." *International Center for the Study of Violent Extremism* (blog), May 2017. http://www.icsve.org/research-reports/isis-drones-evolution-leadership-bases-operations-and-logistics.

Alves, Fabio, and Gamani Karunasiri. "MEMS Acoustic Directional Finder for Small Flying UAS." CRUSER's TechCon, Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/58040.

Asymmetric Warfare Group. *Defense-in-Depth Experiment (DiDEX) 2018 Final Report*. Fort A.P. Hill, VA: Asymmetric Warfare Group, 2019.

Asymmetric Warfare Group. *Defense-in-Depth Experiment (DiDEX) 2018 Observation Report*. Fort A.P. Hill, VA: Asymmetric Warfare Group, 2019.

Bandy, Daniel, Jay Parsons, Aaron Goldan, and Eric Mitchell. "JOKTAK: Joint Operations Center Tactical Assault Kit." Defense Analysis poster, Naval Postgraduate School, 2018.

Beall, Ryan. *Windtalker Overview*. Mountain View, CA: Defense Innovation Unit, 2019.

Bein, Doina. "Self-Configuring, Self-Organizing, and Self-Healing Schemes in Mobile Ad Hoc Networks." In *Guide to Wireless Ad Hoc Networks*, edited by Sudip Misra, Isaac Woungang, and Subhas Misra, 27-41. London: Springer Science and Business Media, 2009.

Butterworth-Hayes, Philip. "Special Report—U.S. Department of Defense Spending on Counter-UAS Reaches USD 1.5 Billion in 2018." *Unmanned Airspace* (blog), November 4, 2018. https://www.unmannedairspace.info/counter-uas-systems-and-policies/special-report-us-department-defense-spending-counter-uas-reaches-usd-1-5-billion-2018/.

CNN. "Russian Airbase Attacked by Drones in Syria." August 16, 2018. Video, 1:46. https://www.cnn.com/videos/world/2018/08/16/drone-attacks-russian-forces-aleppo-syria-pleitgen-lkl-vpx.cnn.

Coursey, Todd. "MEMS Acoustic Sensor for Drone Detection." Presentation at Naval Postgraduate School, Monterey, CA, April 11, 2017. https://calhoun.nps.edu/handle/10945/53349.

Department of the Army. *Counter-Unmanned Aircraft System Techniques*. ATP 3-01.81. Washington, DC: Department of the Army, 2017. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3099_ATP%203-01x81%20FINAL%20WEB.pdf

Department of the Army. *Mission Command*. ADP 6-0. Washington, DC: Department of the Army, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN19189_ADP_6-0_FINAL_WEB_v2.pdf.

Department of the Army. *Protection*. ADP 3-37. Washington, DC: Department of the Army, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18685_ADP%203-37%20FINAL%20WEB_v2.pdf.

Ferriter, Michael, Phil Schupp, and Sverre Wetteland. "Organizing Chaos: The Tactical Assault Kit Collaborative Mission Planner." Master's Thesis, Naval Postgraduate School, 2017. http://hdl.handle.net/10945/56915.

Fioranelli, Francesco, M. Ritchie, H. Griffiths, and H. Borrion. "Classification of Loaded/Unloaded Micro-Drones Using Multistatic Radar." *Electronics Letters* 51, no. 22 (2015): 1813-15. https://doi.org/10.1049/el.2015.3038.

Fu, H., S. Abeywickrama, L. Zhang, and C. Yuen. "Low-Complexity Portable Passive Drone Surveillance via SDR-Based Signal Processing." *IEEE Communications Magazine* 56, no. 4 (April 2018): 112-18. https://doi.org/10.1109/MCOM.2018.1700424.

Ganti, Sai Ram, and Yoohwan Kim. "Implementation of Detection and Tracking Mechanism for Small UAS." In *International Conference on Unmanned Aircraft Systems* (2016): 1254-60, 2016. https://doi.org/10.1109/ICUAS.2016.7502513.

Gettinger, Dan. "Drones Operating in Syria and Iraq." *Center for the Study of the Drone at Bard College* (blog), December 2016. https://dronecenter.bard.edu/files/2016/12/Drones-in-Iraq-and-Syria-CSD.pdf.

Gibbons-Neff, Thomas. "ISIS Drones Are Attacking U.S. Troops and Disrupting Airstrikes in Raqqa, Officials Say." *Washington Post*, June 14, 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say.

Grier, Peter. "April 15, 1953." *Air Force Magazine*, June 2011. http://www.airforcemag.com/MagazineArchive/Documents/2011/June%202011/0611april.pdf.

Guvenc, Ismail, Ozgur Ozdemir, Yavuz Yapici, Hani Mehrpouyan, and David Matolak. "Detection, Localization, and Tracking of Unauthorized UAS and Jammers." In *IEEE/AIAA 36th Digital Avionics Systems Conference* (2017): 1-10. https://doi.org/10.1109/DASC.2017.8102043.

Harper, Jon. “Military, Industry Gung-Ho on Software Defined Radios.” *National Defense*, February 15, 2019. https://www.nationaldefensemagazine.org/articles/2019/2/15/military-industry-gung-ho-on-software-defined-radios.

Harvey, Brendan, and Siu O’Young. “Acoustic Detection of a Fixed-Wing UAV.” *Drones* 2, no. 1 (2018): 1-18. https://doi.org/10.3390/drones2010004.

Hogue, Daniel, and Sarah Gregory. “MEMS-Based Waste Vibrational Energy Harvesters.” Master’s thesis, Naval Postgraduate School, 2013. https://calhoun.nps.edu/handle/10945/34678.

Imperial War Museums. “What Was The ‘Dowding System’?” Last modified June 18, 2018. http://www.iwm.org.uk/history/what-was-the-dowding-system.

King, Stephen. *The Colorado Kid*. New York: Dorchester Publishing Co., 2005.

Kristan, Michael, Jeffrey Hamalainen, Patrick Newell, and Douglas Robbins. *Cursor-on-Target Message Router User’s Guide*. Report Number MP090284. Bedford, MA: MITRE Corporation, 2009. https://doi.org/10.21236/ADA640597.

Lachow, Irving. “The Upside and Downside of Swarming Drones.” *Bulletin of the Atomic Scientists* 73, no. 2 (2017): 96-101. https://doi.org/10.1080/00963402.2017.1290879.

Loo, Jonathan, Jaime Lloret Mauri, and Jesus Hamilton Ortiz. *Mobile Ad Hoc Networks: Current Status and Future Trends*. Boca Raton, Florida: CRC Press, 2012.

MEMS Exchange. “MEMS and Nanotechnology Applications.” Accessed February 7, 2019. https://www.mems-exchange.org/MEMS/applications.html.

Mendis, G. J., T. Randeny, Jin Wei, and A. Madanayake. “Deep Learning Based Doppler Radar for Micro UAS Detection and Classification.” In *IEEE Military Communications Conference* (2016): 924-29. https://doi.org/10.1109/MILCOM.2016.7795448.

Nguyen, Phuc, Mahesh Ravindranatha, Anh Nguyen, Richard Han, and Tam Vu. “Investigating Cost-Effective RF-Based Detection of Drones.” In *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use* (2016): 17-22. https://doi.org/10.1145/2935620.2935632.

O’Donnell, Robert. *RES.LL-001 Introduction to Radar Systems*. Massachusetts Institute of Technology: MIT OpenCourseWare, 2007. https://ocw.mit.edu/resources/res-ll-001-introduction-to-radar-systems-spring-2007.

Persistent Systems. “MPU5: The World’s First Smart Radio.” 2017. https://www.persistentsystems.com/site/wp-content/themes/persistensystems/pdf/mpu5/mpu5_spec_sheet.pdf.

Poitevin, P., M. Pelletier, and P. Lamontagne. “Challenges in Detecting UAS with Radar.” In *International Carnahan Conference on Security Technology* (2017): 1-6. https://doi.org/10.1109/CCST.2017.8167852.

Pullen, John Patrick. “This Is How Drones Work.” *Time*, April 3, 2015. https://time.com/3769831/this-is-how-drones-work.

Quevedo, Á D. de, F.I. Urzaiz, J.G. Menoyo, and A.A. López. “Drone Detection With X-Band Ubiquitous Radar.” In *19th International Radar Symposium* (2018): 1-10. https://doi.org/10.23919/IRS.2018.8447942.

Rassler, Don. “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology.” *Combating Terrorism Center at West Point*, October 20, 2016. https://ctc.usma.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology.

Richards, John Alfred. *GMTI Radar Minimum Detectable Velocity*. Report Number SAND2011-1767. Albuquerque, NM: Sandia National Laboratories, 2011. https://doi.org/10.2172/1011708.

Rubenstein, M., C. Ahler, and R. Nagpal. “Kilobot: A Low Cost Scalable Robot System for Collective Behaviors.” In *IEEE International Conference on Robotics and Automation* (2012): 3293-98. https://doi.org/10.1109/ICRA.2012.6224638.

Saab Solutions. “Giraffe 1X Short Range 3D Radar.” Accessed June 18, 2019. https://saab.com/air/sensor-systems/ground-based-air-defence/giraffe-1x.

Schneider, Tobias, and Theresa Lutkefend. “Nowhere to Hide: The Logic of Chemical Weapon Use in Syria.” *Global Public Policy Institute Study* (blog), February 2019. https://www.gppi.net/media/GPPi_Schneider_Luetkefend_2019_Nowhere_to_Hide_Web.pdf.

Sims, Alyssa. “The Rising Drone Threat from Terrorists.” *Georgetown Journal of International Affairs* 19, no. 1 (2018): 97-107. https://doi.org/10.1353/gia.2018.0012.

Squarehead Technology. “Discovair: Acoustic Drone Detection.” October 2018. https://www.sqhead.com/wp-content/uploads/2018/10/Drone-Detection-Discovair-G2-brochure.pdf.

Squarehead Technology. “Squarehead Unveils Discovair G2.” *Squarehead News* (blog), August 3, 2018. https://www.sqhead.com/squarehead-unveils-discovair-g2.

Stalinsky, Steven, and R. Sosnow. "A Decade Of Jihadi Organizations' Use Of Drones - From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones." *Middle East Media Research Institute*, Inquiry and Analysis Series 1300 (February 21, 2017). https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda.

Tactical Assault Kit. "What is TAK?" Accessed February 7, 2019. https://takmaps.com.

Tadjdeh, Yasmin. "Islamic State Militants in Syria Now Have Drone Capabilities." *National Defense*, August 28, 2014. https://www.nationaldefensemagazine.org/articles/2014/8/28/islamic-state-militants-in-syria-now-have-drone-capabilities.

Thielenhaus, Christopher, and Eric Roles. "Maximizing the Utility of Special Warfare: The Remote Advise and Assist Concept." Master's thesis, Naval Postgraduate School, 2016.

U.S. Special Operations Command. "About USSOCOM: Mission Statement and Vision." June 12, 2019. https://www.socom.mil/about.

Votel, Joseph. *Special Operations Forces Operating Concept: A Whitepaper to Guide Future SOF Development*. Tampa, FL: U.S. Special Operations Command, 2016. https://nsiteam.com/social/wp-content/uploads/2017/01/SOF-Operating-Concept-v1-0_020116-Final.pdf.

Wilmott, Daniel, Fabio Alves, and Gamani Karunasiri. "Bio-Inspired Miniature Direction Finding Acoustic Sensor." *Nature Scientific Reports* 6, no. 29957 (2016). https://www.nature.com/articles/srep29957.

Wilson, J.R.. "The New World of Counter-Drone Technology." *Military and Aerospace Electronics*, November 1, 2018. https://www.militaryaerospace.com/articles/print/volume-29/issue-11/special-report/the-new-world-of-counter-drone-technology.html.

Yayla, Ahmet S, and Anne Speckhard. "The Potential Threats Posed by ISIS's Use of Weaponized Air Drones and How to Fight Back." *International Center for the Study of Violent Extremism* (blog), March 1, 2017. https://www.icsve.org/the-potential-threats-posed-by-isiss-use-of-weaponized-air-drones-and-how-to-fight-back.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California